Energy Research and Development Division
FINAL PROJECT REPORT

SMART GRID INFORMATION ASSURANCE AND SECURITY TECHNOLOGY ASSESSMENT

Prepared for: California Energy Commission
Prepared by: California State University Sacramento

SACRAMENTO STATE
Leadership begins here.

DECEMBER 2010
CEC-500-2013-056

PREPARED BY:

Primary Author(s):

Isaac Ghansah, Ph.D

California State University Sacramento.
6000 J Street
Sacramento, CA 95819-6021
916-278-7659
www.csus.edu

Contract Number: CEC-500-2008-027

Prepared for:

California Energy Commission

David Chambers
Contract Manager

Fernando Piña
Office Manager
Energy Systems Research Office

Laurie ten Hope
Deputy Director
ENERGY RESEARCH AND DEVELOPMENT DIVISION

Rob Oglesby
Executive Director

ACKNOWLEDGEMENTS

The final report, Smart Grid Information Assurance and Security Technology Assessment was prepared with contributions from the following members:

- Prakarn Asavachivanthornkul — Dept. Of Computer Science, CSUS.
- Tina Celia John — Dept. Of Computer Science, CSUS.
- Sandeep Pedditi — Dept. Of Computer Science, CSUS.
- Sumaya Sweha — Dept. Of Computer Science, CSUS.
- Manpreet Randhawa — Dept. Of Computer Science, CSUS.
- Aditi Dave — Dept. Of Computer Science, CSUS.
- Raksha SR — Computer Engineering, CSUS.
- Pooja Ramesh — Dept. Of Computer Science, CSUS.
- Vinod Thirumurthy — Computer Engineering, CSUS.
- Adithya Shreyas — Computer Engineering, CSUS.
- Mithila Paranjpe — Dept. Of Computer Science, CSUS.
- Mayur Anand — Dept. Of Computer Science, CSUS.
- Alan Jones — Listcon
- Robert Hassanali — Listcon

PREFACE

The California Energy Commission Energy Research and Development Division supports public interest energy research and development that will help improve the quality of life in California by bringing environmentally safe, affordable, and reliable energy services and products to the marketplace.

The Energy Research and Development Division conducts public interest research, development, and demonstration (RD&D) projects to benefit California.

The Energy Research and Development Division strives to conduct the most promising public interest energy research by partnering with RD&D entities, including individuals, businesses, utilities, and public or private research institutions.

Energy Research and Development Division funding efforts are focused on the following RD&D program areas:

- Buildings End-Use Energy Efficiency
- Energy Innovations Small Grants
- Energy-Related Environmental Research
- Energy Systems Integration
- Environmentally Preferred Advanced Generation
- Industrial/Agricultural/Water End-Use Energy Efficiency
- Renewable Energy Technologies
- Transportation

Smart Grid Information Assurance and Security Technology Assessment is the final report for the Smart Grid Information Assurance and Security Technology Assessment project (Contract Number 500-08-027) conducted by Center for Information Assurance and Security (CIAS) at California State University Sacramento (CSUS). The information from this project contributes to the Energy Research and Development Division's Energy Systems Integration Program.

For more information about the Energy Research and Development Division, please visit the Energy Commission's website at www.energy.ca.gov/research/ or contact the Energy Commission at 916-327-1551.

ABSTRACT

This report addresses cyber security and privacy issues in the emerging Smart Grid, specifically:

1. Identifying and grouping potential issues affecting the confidentiality, integrity, and availability of information flow.
2. Investigating which information security best practice(s) apply to the Smart Grid and to what extent they can they be applied to mitigate actions that violate confidentiality, integrity, and the availability of information.
3. Exploring possible cyber security research and development issues that should be addressed.
4. Identifying and recommending which potential research and development efforts should and should not be confidential.
5. Identifying technical and non-technical solutions to ensure the privacy of end user information.

The researchers used information from various Smart Grid working groups dealing with cyber security issues as well as web sources, journals, and magazines.

This project demonstrated that although the Smart Grid has several potentially significant vulnerabilities, information security best practices can be used for mitigating some of them. The researchers also identified additional areas needing research. The researchers found that with a few exceptions, the research processes and results should be non-confidential.

Finally, the researchers addressed a number of privacy issues associated with information gathered within the Smart Grid, such as meter data and customers' information. Access to this sensitive information could violate customers' privacy by exposing personal information, energy consumption use and patterns and other activities customers' homes. Existing privacy laws and regulations with respect to smart meter data are also discussed.

Because Smart Grid systems will collect and transmit different kinds of information, best practices and data handling practices can be applied to mitigate privacy issues. Nevertheless, there are some issues regarding privacy laws and regulations, privacy on the web, and privacy for inference and aggregation that should be taken into consideration and require further research.

Keywords: Public Interest Energy Research, PIER, smart grid, electric grid, cyber security, critical infrastructure, information assurance, research, development, privacy.

Please use the following citation for this report:

Ghansah, Isaac, 2010. *Smart Grid Information Assurance and Security Technology Assessment*, California Energy Commission, PIER Energy-Related Environmental Research Program. CEC-500-2013-056

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

Introduction

Attempts to combine advancements in information technology with electricity infrastructure allowing the electric system to become "smart" have been increasing in recent years. The challenges of improving the reliability of the electricity system, integrating renewable resources such as solar and wind farms into the electricity network, offering customer options to reduce electricity consumption, and distributing electricity more effectively have made the Smart Grid more attractive. The United State government and several states including California have legislation backing the development of the Smart Grid. There is also interest in the Smart Grid from several countries across the globe. To accelerate these developments, NIST (National Institute of Standards and Technology) is working on developing interoperability standards for the Smart Grid through a community of Smart Grid stakeholders. Both the California Energy Commission (CEC) and the California Public Utilities Commission (CPUC) have also launched plans to modernize the electric grid in California. The Smart Grid system uses interconnected elements that optimize communications and control across the different segments of energy generation, distribution, and consumption. Unfortunately, because of the critical nature of the technology, the complexity of the Smart Grid, and the services that it provides, the grid could become a prime target for acts of terrorism and cyber attacks. Privacy issues in the Smart Grid also need to be addressed since customer information collected by utilities or transferred in Smart Grid systems could be exploited, resulting in the exposure of consumers' energy consumption uses and patterns, as well as their personal information. Potential vulnerabilities and risks need to be identified and researched to mitigate these vulnerabilities since no system is 100% secure.

This report discusses Smart Grid cyber security issues and addresses security controls and countermeasures to mitigate those risks using information security best practices. Where best practices are not adequate, the researchers suggested research topics that need to be addressed to help solve those problems, as well as identified which research and development (R&D) results and processes should be confidential or non-confidential. Privacy concerns and best practices to mitigate them in the Smart Grid are also addressed.

Project Purpose

The Center for Information Assurance and Security (CIAS) and the California Smart Grid Center (CSGC) at Sacramento State University completed this project and prepared this report at the request of the California Energy Commission (CEC) Public Interest Energy Research (PIER) program. The main goal of the original agreement was determining information assurance, security, and privacy issues associated with Smart Grid infrastructure and recommending R&D priorities in those areas. Another goal was identifying information security best practices that can be applied to the Smart Grid system and R&D issues that should be addressed.

Project Results

To achieve these objectives the researchers:

- Participated and in some cases coordinated conference calls and face-to-face meetings with Smart Grid and cyber security experts.
- Attended workshops on demand response research, smart grid cyber security standards, and smart grid interoperability.
- Performed an online literature search.
- Informally interviewed some utility experts on electricity generation, transmission, and distribution processes.

This report identified potential threats, vulnerabilities, and risks of the following major Smart Grid components: advanced metering infrastructure, demand response systems, home area networks (HANs), neighborhood area networks that connect the home to utility systems, Supervisory Control and Data Acquisition (SCADA) systems that are used for controlling generation, transmission and distribution systems, and plug-in electric vehicles. The researchers also addressed information security best practices for dealing with cyber security vulnerabilities and threats to the Smart Grid in general as well as to the specific components mentioned above.

Finally, the researchers addressed privacy issues associated with information gathered within the Smart Grid, identified best practices for dealing with privacy concerns, and discussed potential research topics to deal with areas where best practices are inadequate.

The results showed that the Smart Grid has a number of potentially significant cyber security issues that must be addressed. These issues included confidentiality of user information, integrity of demand response systems, integrity and availability of SCADA (grid) systems, and integrity and availability of plug-in electric vehicles (PEVs). The researchers also addressed communication system cyber security issues.

The researchers found that in some cases information security best practices used in conventional IT systems can be used to address Smart Grid vulnerabilities. Although they can be used directly in some cases (e.g., security policy creation), there are other situations where they cannot. Additionally, there are situations (e.g., intrusion detection) where, because of the unique characteristics of Smart Grid critical infrastructure, further research is needed to address security issues in those unique cases.

As indicated in the report, the researchers found that most of the research on Smart Grid cyber security was non-confidential, although in very few cases the results of the research should be held confidential. An example is where vulnerability assessment or penetration testing (a red team exercise) is performed on the Smart Grid system, where the information should be released only on a need-to-know basis.

Project Benefits

The benefits of this project for California included:

- Increased customer trust of the Smart Grid.
- Increased regulator understanding of the security issues in the Smart Grid that need to be addressed by manufacturers and utilities.
- Increased understanding of the privacy issues in the Smart Grid and how they can be addressed.
- Because the project identified security and privacy issues in the Smart Grid infrastructure and proposed solutions and research areas, the results will ultimately enable the wide deployment and acceptance of the Smart Grid, resulting in increased energy efficiency and lower energy costs.

CHAPTER 1:
Introduction

This document, Smart Grid Information Assurance and Security Technology Assessment, contains the Comprehensive Smart Grid Security Issues, Best Practices, Research and Development and Privacy Issues researched by Smart Grid Research Group which is part of the California Smart Grid Center (CSCG) and the Center for Information Assurance and Security (CIAS) at California State University Sacramento (CSUS). This report contains the results of research tasks specified in a statement of work for the California Energy commission as follows:

1. Identify the potential issues affecting the confidentiality, integrity, and availability of information flow in the Smart Grid system. For instance, hacker/terrorist use of malicious software to perform denial of service attacks on critical infrastructure such as the Smart Grid will be examined. Group the issues with respect to confidentiality, integrity, and availability.
2. Investigate which information security best practice(s) apply to smart grid and to what extent can they be applied. Best practices such as use of firewalls for perimeter defense, intrusion detection, incident response handing, defense in depth, etc. are well known in the information security arena. These best practices are intended to mitigate actions that violate confidentiality, integrity, and availability of the information flow in the smart grid.
3. Explore possible cyber security R&D issues that should be addressed in Smart Grid. Some of these could involve wireless sensors, wireless communication systems, monitoring, and incident response systems.
4. Identify and recommend which potential R&D efforts should and should not be confidential.
5. Identify technical and non-technical solutions to ensure the privacy of end user information. Because Smart Grid systems will contain end user information, privacy is critical.

The above tasks are covered in the various chapters of the documents as follows:

1. The second chapter describes potential Smart Grid Information Assurance and Security issues. Issues specifically addressed in this chapter are potential threats, vulnerabilities and risks. Most of the information in this chapter is currently being discussed in the NIST Bottom-up Security Group which is subgroup within the NIST Smart Grid Cyber Security Coordination Task Group (CSCTG). This chapter is about the task one listed above.
2. The third chapter is about information security best practices that can be used to deal with smart grid threats, vulnerabilities and risks. That is, it covers mitigation and countermeasures to address those vulnerabilities. Unless otherwise stated the terms mitigation, countermeasure and best practices are used interchangeably in this

document. The vulnerabilities were covered in the second chapter, Smart Grid Cyber Security Potential Threats, Vulnerabilities and Risks. This chapter is about the task two listed above.

3. The fourth chapter discusses a number of potential research and development topics for Smart Grid cyber security. The best practices suggested in the chapter 3, Best Practices for Handling Smart Grid Cyber Security, provided solutions to several threats, but there were still areas where the solutions were not adequate. This chapter not only discusses the research and development issues for cyber security in the Smart Grid, but also specifies whether the processes for conducting a specific R&D in smart grid cyber security and the results thereof should be publicly disseminated or not. This chapter is about tasks three and four listed above.
4. The fifth chapter addresses privacy issues related to information gathered within Smart Grid. It also identifies best practices for privacy concerns in the Smart Grid as well as specifies potential research topics related to the privacy in the Smart Grid. This chapter is about the task five listed above.
5. The sixth chapter concludes the document.

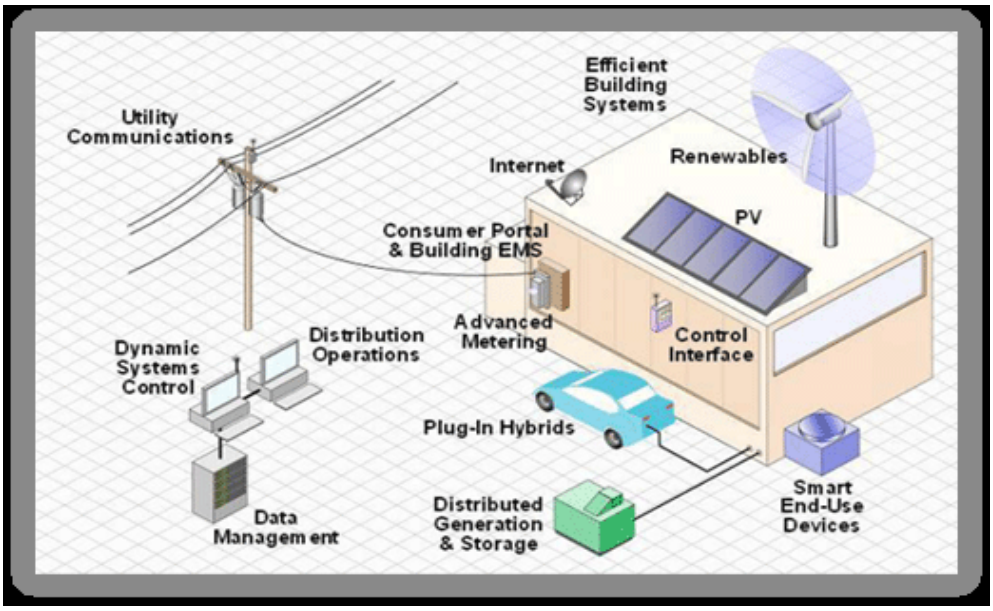
1.1 What is Smart Grid?

A smart grid (See Figure 1-1 and Figure 1-2) delivers electricity from suppliers to consumers using digital technology to save energy, reduce cost and increase reliability and transparency. It is a modernized electricity network which is being utilized as a way of addressing energy independence, global warming and emergency resilience issues.[1]

The primary components of Smart Grid are shown in Figure 1-1. Figure 1-2 explains how the Smart Grid works.

[1] Wikipedia, "Smart Grid". [online] Available: http://en.wikipedia.org/wiki/Smart_grid.

Figure 1-1: Smart Grid Network[2]



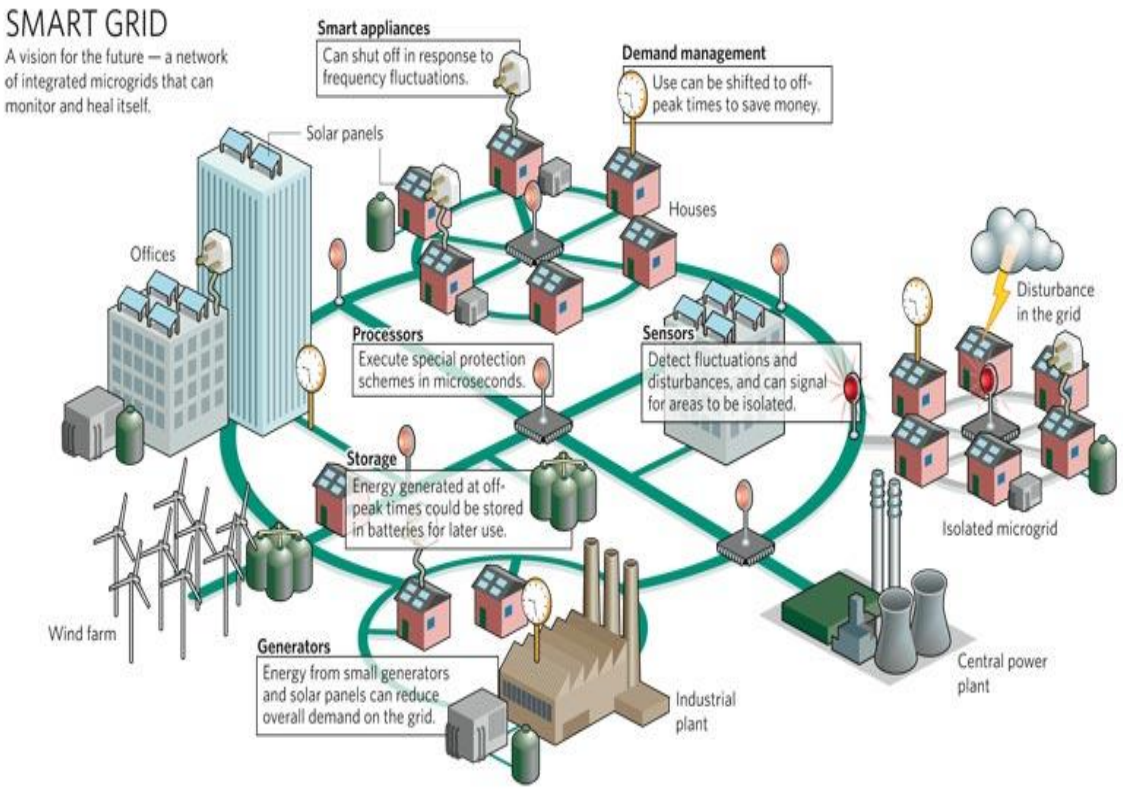
Smart Grid has the following characteristics[3]

- Self-healing from power disturbance events
- Enabling active participation by consumers in demand response
- Operating resiliently against physical and cyber attack
- Providing power quality for 21st century needs
- Accommodating all generation and storage options
- Enabling new products, services, and markets
- Optimizing assets and operating efficiently

[2] L. Bruno; Innovation Pipeline, "Federal Stimulus and Cleantech Infrastructure". [online] Available: http://www.larta.org/lartavox/articles/5-2009/Federal-Stimulus-and-Cleantech-Infrastructure.htm

[3] National Energy Technology Laboratory for the Department of Energy Office of Electricity Delivery and Energy Reliability, "A Vision for the Smart Grid", June 2009. [online] Available: http://www.netl.doe.gov/smartgrid/referenceshelf/whitepapers/Whitepaper_The%20Modern%20Grid%20Vision_APPROVED_2009_06_18.pdf.

Figure 1-2: Smart Grid Working[4]



Technically, the Smart Grid is unique in many respects. First by its nature the Smart Grid is a complex system. Second, Smart Grid is one of 18 critical infrastructures identified by DHS. These critical infrastructure systems are so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof.[5] Third, smart grid is a large system because it is used to control electricity which is present is almost every home. Fourth smart grid is a 'special' critical infrastructure because many of the 18 critical infrastructures depend on it. For instance, electricity is needed by banks, emergency services such as hospitals, telecommunications, computers, etc. Indeed, the Cyber Security Strategy for the 44th President of the United States cites energy, financial, Information Technology (IT), and telecommunications as the four critical infrastructures with the most critical cyber assets.

[4] D. Heyerman, "The Smart Grid Frontier: Wide Open", May 3, 2009. [online] Available: http://tinycomb.com/2009/05/03/what-is-the-smart-grid/

[5] DHS Website, "Critical Infrastructure and Key Resources". [online] Available: http://www.dhs.gov/files/programs/gc_1189168948944.shtm

The unique characteristics of smart grid stated above are the reasons why cyber security of the smart grid is imperative. The smart grid has many anticipated benefits.[6]

- Improves power reliability and quality
- Optimizes facility utilization and averts construction of back-up (peak load) power plants
- Enhances capacity and efficiency of existing electric power networks
- Improves resilience to disruption
- Enables predictive maintenance and "self-healing" responses to system disturbances
- Facilitates expanded deployment of renewable energy sources
- Accommodates distributed power sources
- Automates maintenance and operation
- Reduces greenhouse gas emissions by enabling electric vehicles and new power sources
- Reduces oil consumption by reducing the need for inefficient generation during peak usage periods
- Improves cyber security
- Enables transition to plug-in electric vehicles and new energy storage options
- Increases consumer choice

Because of its many benefits the federal government and many other state governments including California, are funding research and demonstration efforts for the smart grid. Both US departments of commerce and energy are pushing for interoperability standards for smart grid. NIST, as a branch of the commerce department is leading the effort to create those standards. Additionally, organizations as diverse as Electric Utilities, US DOE, NIST, Google, Microsoft, GE, IEEE, NERC, FERC, IEC, and ANSI have published documents about Smart Grid.

Major reasons for this cyber security research are because of the complexity of the smart grid, the importance of the smart grid as a super-critical infrastructure, and the fact that many reports of potential attacks on the grid have been disseminated in the media. This research should help put some of these media reports in perspective. However, the primary purpose of this current report is to discuss threats and vulnerabilities, and general security problems; address controls and countermeasures to mitigate those risks, using best practices; and where best practices are not adequate the researchers will suggest research topics that need to be addressed in the future to help solve those problems. This report also addresses privacy issues in the Smart Grid.

---

[6] Office of the National Coordinator for Smart Grid Interoperability, NIST Special Publication 1108, "NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0". [online] Available: http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf

1.2 Report Organization

This document is organized as follows:

- **Chapter 2:** *Smart Grid Cyber Security Potential Threats, Vulnerabilities and Risks*
    - Examples of reported vulnerabilities of the smart grid are first introduced in Section 2.1.
    - Information assurance and security concepts and terminologies that are used throughout the document are discussed in Section 2.2.
    - Security issues of important smart grid components, namely Advance Metering Infrastructure, Demand Response, Customer Domain Systems (i.e. Home Area Networks, Gateways, and Neighborhood Area Networks), Supervisory Control and Data Acquisition and Distributed Network Protocol, and Plug in Electric Vehicles are discussed in Section 2.3 through 2.7.
    - Important security issues that are critical in smart grid but that do not fit cleanly in the above smart grid components are included in Section 2.8. Most of the issues listed in Section 2.8 are research topics that will be discussed in more detail in Chapter 4.
- **Chapter 3:** *Best Practices for Handling Smart Grid Cyber Security*
    - Information security best practices for Smart Grid Cyber Security, which includes general best practices for securing IT systems; system life cycle management; technical best practices for ensuring security requirements of confidentiality, integrity, availability, and accountability; and secure systems design principles, are introduced in Section 3.1 and referred throughout the document in subsequent Sections and Chapters.
    - Mitigation and countermeasures as well as best practices to address security issues and vulnerabilities of important smart grid components discussed in Chapter 2, namely Demand Response, Customer Domain (i.e. Home Area Networks, Gateways, and Neighborhood Area Networks), Advanced Metering Infrastructure, Supervisory Control and Data Acquisition and Distributed Network Protocol, Plug in Electric Vehicles, and Distributed Energy Resources. This is discussed in Section 3.2 through 3.7.
- **Chapter 4:** *Identifying and Categorizing Research and Development Issues for Cyber Security in the Smart Grid*
    - Introduction to research and development and the organization of potential research topics are introduced in Section 4.1.
    - General research topics, which could be applied to different components of the smart grid systems, and categorization of these topics into confidential or non-confidential, are discussed in Section 4.2.

- Potential research topics with respect to cryptography and key management, which could be implemented in the Smart Grid, and categorization of these topics into confidential or non-confidential, are discussed in Section 4.3.
- Specific domain topics for important smart grid components, including Demand Response, Customer Domain (i.e. Home Area Networks, Gateways, and Neighborhood Area Networks), Advanced Metering Infrastructure, Supervisory Control and Data Acquisition and Distributed Network Protocol, and Plug in Electric Vehicles, and categorization of these topics into confidential or non-confidential, are discussed in Section 4.4.
- Research topics, which are related to wireless communication security , and categorization of these topics into confidential or non-confidential, are discussed in Section 4.5

- **Chapter 5:** *Smart Grid and Privacy*
  - Introduction to privacy, definitions of privacy and principles of privacy in the Smart Grid are introduced in Section 5.1.
  - Smart Grid and privacy concerns, risks, and privacy laws associated with the smart grid data are discussed in Section 5.2.
  - Best Practices to limit the violations to the privacy of customers' information are provided in Section 5.3.
  - Research topics with respect to privacy issues for the Smart Grid, are discussed in Section 5.4.
- **Chapter 6:** *Conclusion*
- **Appendix**
  - Appendix A is a list of Use Cases for the various components of the Smart Grid and corresponding Cyber security requirements. It is part of NISTIR 7628.[7] The Appendix can be viewed as an introductory document which highlights a number of the cyber security issues discussed in Chapter 2 of this report.

[7] Office of the National Coordinator for Smart Grid Interoperability, NIST Special Publication 1108, "NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0". [online] Available: http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf.

CHAPTER 2:
Smart Grid Cyber Security Potential Threats, Vulnerabilities and Risks

2.1 Reported Vulnerabilities of Smart Grid

This section cites a number of smart grid vulnerabilities reported in the media and elsewhere. The intent is to bolster the reason for this research.

Most of the nation's electricity system was built when primary energy was relatively inexpensive. Grid reliability was mainly assured by having excess capacity in the system, with unidirectional electricity flow to consumers from centrally dispatched, coal-fired power plants. Recognizing these challenges, the energy community is starting to combine advancements in information technology with electricity infrastructure, allowing the electric system to become "smart." This system uses interconnected elements that optimize the communications and control across the different segments of energy generation, distribution, and consumption. But the unfortunate reality is that because of the critical nature of the technology and the services that it provides, the grid becomes a prime target for acts of terrorism and cyber attacks.[8]

The Smart Grid has several layers and every network layer and technology used represents a potential avenue of attack. The legacy grid already uses many different communication paths and protocols to connect utility operation centers with system operators such as Independent Service Operators (ISOs) and Regional Transmission Operators (RTOs). A wide variety of data transfer protocols are used. Most existing protocols have some form of vulnerability or another. Advanced meter infrastructure and its network of smart meters provide a foundation for smart grid. Research firm Parks Associates estimates that 8.3 million smart meters have been installed in US homes, about 6% penetration. These meters must be accessible for ongoing maintenance and operations. Once a meter is compromised it can be used to attack other parts of the network. Smart thermostats, in-home displays, appliances, charging stations and various plug-loads are connected together by an Energy Management System (EMS) application running on the Home Area Network (HAN). Even though these are less likely to be used in large-scale assaults they represent vulnerability for tampering with meter data and the related customer billing. Transmission and distribution substations contain many power control devices such as circuit breakers, transformers, capacitors, and monitoring devices. The smart grid increases the level of automation in substations and with this increase, the number of electronic control elements increases the potential vulnerabilities. Smart Grid uses new sensors which will enhance the situational awareness of the grid and enable operators to react to power anomalies more quickly but sensor network itself opens up an additional line of attack. The operations center is another area of potential attack. Vulnerabilities can exist in the utility enterprise

[8] Cisco Smart Grid, Solutions for the next Generation Energy Network: http://www.cisco.com/web/strategy/docs/energy/aag_c45_539956.pdf

firewall, its enterprise applications, and/or its operator authentication and training systems. This makes the operation center vulnerable to a top-down attack from an intruder or to an insider-attack from a disgruntled employee.[9]

There have been reports from different sources regarding the potential attacks to the Smart Grid. The Department of Homeland Security (DHS) has reported that cyber spies, likely from China and Russia, have managed to inject malicious software into the electric grid, water, sewage, and other infrastructure control software. This software could enable malicious users to take control of key facilities or networks via the Internet, causing power outages and tremendous damage to most sectors of the economy.[10] As the grid becomes more central to our energy infrastructure, it will become more important to ensure its security. Smart Grid systems create a link between physical systems and software systems, both of which can fail.[11] IOActive, a professional security services firm, determined that an attacker with $500 of equipment and materials and a background in electronics and software engineering could "take command and control of the AMI allowing for the en masse manipulation of service to homes and businesses. The Reports from CNN questioned the smartness of Smart Grid to forge ahead with the high technology, digitally based electricity distribution and transmission system. It also reported that the tests have shown that a hacker can break into the system, with some cybersecurity expert's suggestions a massive blackout could result.[12] The American Society for Industrial Security (ASIS) International Chief Security Officer (CSO) Roundtable reported that the electric grid is highly dependent on computer-based control systems. These systems are increasingly connected to open networks such as the internet, exposing them to cyber risks. Any failure of our electric grid, whether intentional or unintentional, would have a significant and potentially devastating impact on our nation. The Wall Street Journal recently reported that cyber spies from China, Russia, and other countries may have penetrated the US electrical grid and implanted software programs that could be used to disrupt the system.[13]

---

[9] Carbon-Pros on August 24, 2009: http://carbon-pros.com/blog1/2009/08/smart_grid_security_vulnerabil.html

[10] Ali Nourai, "Spyware". Smart Grid News. http://www.smartgridnews.com/artman/publish/News_Blogs_News/Foreign_ Cyber-Spies _Inject _Spyware_ into_U_S_Grid_with_Potential_for_Serious_Damage-562.html

[11] Alex Yu Zheng, "Smart Security for Smart Grid: New Threats on the Horizon". Smart Grid News. http://www.smartgridnews.com/artman/publish/Technologies_Security_News/Smart-Security-for-a-Smart-Grid-New-Threats-on-the-Horizon-1226.html

[12] Jeanne Meserve, "Smart Grid may be Vulnerable to Hackers". CNN. http://www.cnn.com/2009/TECH/03/20/smartgrid.vulnerability/index.html

[13] Jude Clemente, "The Security Vulnerabilities of Smart Grid". Journal of Energy Security, June 2009. http://www.ensec.org/index.php?option=com_content&view=article&id=198: the-security-vulnerabilities-of-smart-grid&catid=96:content&Itemid=345

The communications of Association for Computing Machinery (ACM) reported that vulnerabilities in the smart grid also can be caused by inadequate patch, configuration, and change management processes, insufficient access controls, and the failure to create risk assessment, audit, management, and incident response plans. There are also a number of privacy concerns associated with the real-time, two-way communication between consumers and suppliers that the smart grid will allow. One important issue that needs to be dealt with is the data that will be collected automatically from smart meters and how that information will be distributed and used throughout the grid.[14]

The Smart Grid attacks were also tested in laboratories. IOActive have created a worm that could quickly spread among Smart Grid devices, small computers connected to the power grid that give customers and power companies better control over the electricity they use.[15] Yao Liu, Peng Ning from North Carolina State University and Michael K. Reiter from University of North Carolina, Chapel Hill have reported a new class of attacks, called false data injection attacks, against state estimation in electric power grids and they show that an attacker can take advantage of the configuration of a power system to launch such attacks to successfully bypass the existing techniques for bad measurement detection and demonstrated the success of these attacks through simulation using the IEEE 9-bus, 14-bus, 30-bus, 118-bus, and 300-bus systems.[16]

The Smart Grid and related fields have been attacked in the real world. CIA's report from the Associated Press has reported that hackers literally turned out the lights in multiple cities after breaking into electrical utilities and demanding extortion payments before disrupting the power. Reports from Washington Post also claim that the CIA Analysts said cyber attackers have hacked into the computer systems of utility companies outside the United States and made demands, in at least one case causing a power outage that affected multiple cities. The attacker's information was not known but the intrusion came from the Internet.[17] The National Journal Magazine reported that Computer hackers in China, including those working on behalf of the Chinese government and military, have penetrated deeply into the information systems of U.S. companies and government agencies, stolen proprietary information from American executives in advance of their business meetings in China, and, in a few cases, gained access to electric power plants in the United States, possibly triggering two recent and widespread blackouts in Florida and the Northeast. The hacker triggered a cascade effect, shutting down large portions

---

[14] Infoworld, "Smart Grid Vulnerabilities Could Cause Widespread Disruptions". October 2009. http://cacm.acm.org/news/43974-smart-grid-vulnerabilities-could-cause-widespread-disruptions/fulltext

[15] Timothy, "Smart Grid Computers Susceptible to Worm Attack". Slashdot, March 2009. http://hardware.slashdot.org/article.pl?sid=09/03/22/082236

[16] Yao Liu, Peng Ning, Michael K. Reiter. False Data Injection Attacks against State Estimation in Electric Power Grids. Department of Computer Science, North Carolina State University. ftp://ftp.csc.ncsu.edu/pub/tech/2009/TR-2009-5.pdf

[17] Roberto, http://www.cyberpunkreview.com/news-as-cyberpunk/the-cias-latest-claim-hackers-have-attacked-foreign-utilities/ Cyber Punk News, January 2008.

of the Florida power grid which created the Florida Black Out[18]. The interconnected nature of the bulk electric system requires all entities whose operations can affect the operation of the bulk electric system to be as secure from cyber incidents as practicable to ensure bulk electric system reliability. The North American Electric Reliability Corporation (NERC) reported that on January 25, 2003, the SQL Slammer Worm was released by an unknown source. The worm significantly disrupted many Internet services for several hours. It also adversely affected the bulk electric system controls.[19]

Smart Grid will simultaneously expand the infrastructure for transporting electricity and present a more physically challenging infrastructure to protect. Smart Grid's use of internet technologies should have full protection prior to its deployment as it is a matter of national security.[20]

2.2 Information Assurance and Security Concepts and Policies

Information Assurance and Security issues ultimately involve protection of information. Information protection criteria are usually specified in policies such as confidentiality, integrity, and availability. The researchers included accountability as a separate policy even though it can be viewed as Integrity issue because it is critical for the smart grid. NIST has defined these security policies as follows.[21]

2.2.1 Confidentiality

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

The property that sensitive information is not disclosed to unauthorized individuals, entities or processes.

2.2.2 Integrity

Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

Data integrity is the property that data has not been altered in an unauthorized manner. It covers data integrity covers data in storage, during processing, and while in transit and

---

[18] Shane Harris. http://www.nationaljournal.com/njmagazine/cs_20080531_6948.php National Journal Magazine, May 2008.

[19] Charles E. Noble. http://www.nerc.com/docs/standards/Chuck-Noble-RBB-Letter.pdf CISSP Information Security, ISO New England.

[20] Ali Nourai. "Foreign Cyber-Spies Inject Spyware into US Grid." http://www.smartgridnews.com/artman/publish/News_Blogs_News/Foreign_Cyber-Spies_Inject_Spyware_into_U_S_Grid_with_Potential_for_Serious_Damage-562.html. Smart Grid News.

[21] Charles E. Noble. http://www.nerc.com/docs/standards/Chuck-Noble-RBB-Letter.pdf CISSP Information Security, ISO New England.

includes the property that sensitive data has not been modified or deleted in an unauthorized and undetected manner.

2.2.3 Availability

Ensuring there's timely and reliable access to and use of information.

2.2.4 Accountability

Is the security goal that generates the requirement for actions of an entity to be traced uniquely to that entity? This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.

2.2.5 Security Concepts and Smart Grid

With the Smart Grid's transformation of the electric system to a two-way flow of electricity and information, the Information Technology (IT) and telecommunications infrastructures have become critical to the energy sector infrastructure. Therefore, the management and protection of systems and components of these infrastructures must also be addressed by an increasingly diverse energy sector.

IT and telecommunication sectors have existing cyber security standards to address vulnerabilities and assessment programs to identify known vulnerabilities in these systems. These same vulnerabilities need to be assessed in the context of the Smart Grid. In addition, the Smart Grid has additional vulnerabilities due to its complexity, large number of stakeholders, and highly time-sensitive operational requirements.

The following definitions of cyber infrastructure and cyber security from the National Infrastructure Protection Plan (NIPP) and quoted in NISTIR7628 are included to ensure a common understanding.

- Cyber Infrastructure: Includes electronic information and communications systems and services and the information contained in these systems and services. Information and communications systems and services are composed of all hardware and software that process, store, and communicate information, or any combination of all of these elements. Processing includes the creation, access, modification, and destruction of information. Storage includes paper, magnetic, electronic, and all other media types. Communications include sharing and distribution of information. For example: computer systems; control systems (e.g., SCADA); networks, such as the Internet; and cyber services (e.g., managed security services) are part of cyber infrastructure.

For this chapter, cyber security is defined as follows:

- Cyber Security the protection required to ensure confidentiality, integrity and availability of the electronic information communication system.
- Integrity is generally considered the most critical security requirement for power system operations, and includes assurance that:
    - Data has not been modified without authorization
    - Source of data is authenticated

- Timestamp associated with the data is known and authenticated
- Quality of data is known and authenticated

- Availability is generally considered the next most critical security requirement, although the time latency associated with availability can vary:
  - 4 ms for protective relaying
  - Sub-seconds for transmission wide-area situational awareness monitoring
  - Seconds for substation and feeder SCADA data
  - Minutes for monitoring non-critical equipment and some market pricing information
  - Hours for meter reading and longer term market pricing information
  - Days/weeks/months for collecting long term data such as power quality information

- Confidentiality is generally the least critical for actual power system operations, although this is changing for some parts of the power system, as customer information is more easily available in cyber form:
  - Privacy of customer information is the most important
  - Electric market information has some confidential portions
  - General corporate information, such as human resources, internal decision-making, etc.

2.3 Advanced Metering Infrastructure (AMI) Security Issues

2.3.1 Introduction

Advanced Metering Infrastructure (AMI) refers to systems that measure, collect and analyze energy usage, from advanced devices such as electricity meters, gas meters, and/or water meters, through various communication media on request or on a pre-defined schedule. This infrastructure includes hardware, software, communications, customer associated systems and meter data management (MDM) software.[22]

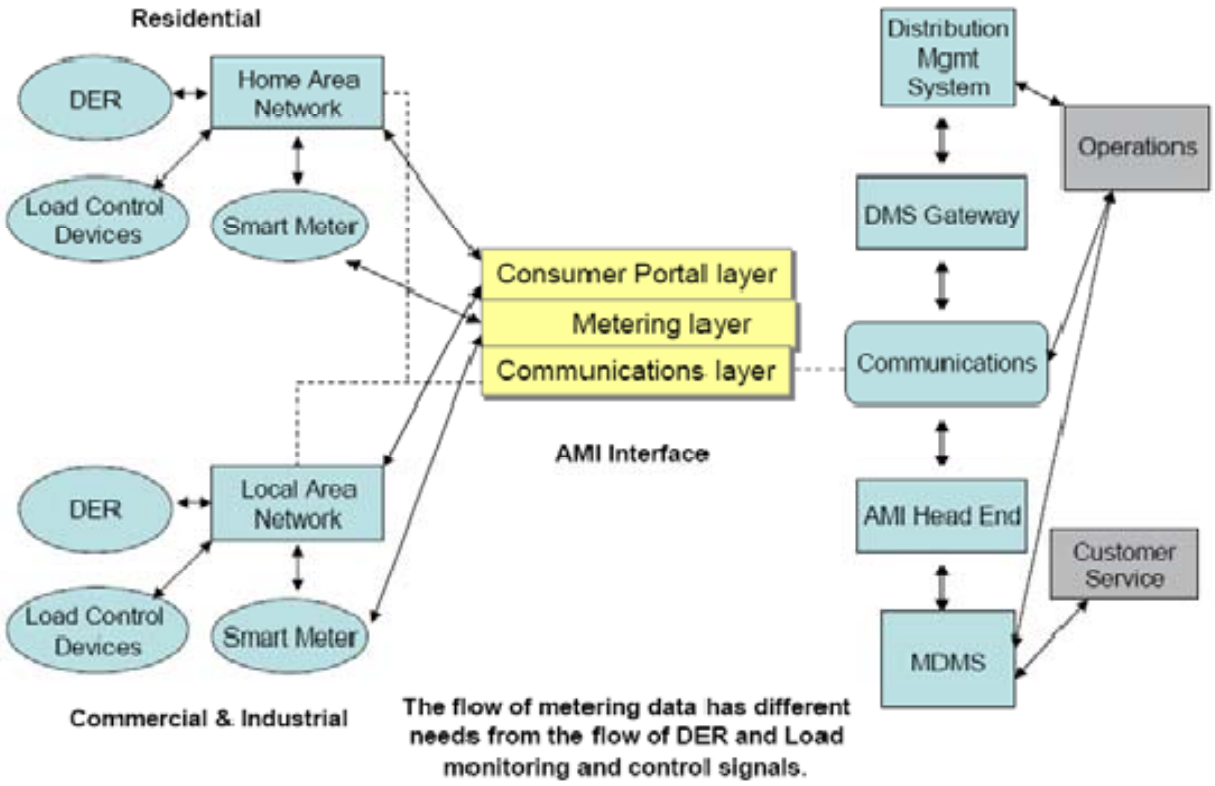
The network between the measurement devices and business systems allows collection and distribution of information to customers, suppliers, utility companies and service providers. This enables these businesses to either participate in, or provide, demand response solutions, products and services. By providing information to customers, the system assists a change in energy usage from their normal consumption patterns, either in response to changes in price or

[22] Wikipedia; Advanced Metering Infrastructure; Available [Online]: http://en.wikipedia.org/wiki/Advanced_Metering_Infrastructure

as incentives designed to encourage lower energy usage use at times of peak-demand periods or higher wholesale prices or during periods of low operational systems reliability.
AMI systems are viewed as consisting of the following components (see also Figure 2-1):[23]

- Smart Meter – The smart meter is the source of metrological data as well as other energy-related information. These smart meters can provide interval data for customer loads as well as distributed generation.
- Customer Gateway – The customer gateway acts as an interface between the AMI network and customer systems and appliances within the customer facilities, such as a Home Area Network (HAN) or Building Management System (BMS). It may or may not co-locate with the smart meter.
- AMI Communications Network – This network provides a path for information to flow from the meter to the AMI head end.
- AMI Head End – This system manages the information exchanges between external systems, such as the Meter Data Management (MDM) system and the AMI network.

Figure 2-1: AMI Components



Source: Open Smart Grid; Shared Documents;

[23] Open Smart Grid; Shared Documents; Available [Online]: http://osgug.ucaiug.org/Shared%20Documents/Forms/AllItems.aspx

2.3.2 AMI Security Threats [24]

The following types of security threats are possible on AMI of Smart Grid:

- **Eavesdropping:** It is unauthorized real-time interception of a private communication.
- **Traffic Analysis:** It is the process of intercepting and examining messages in order to deduce information from patterns in communication.
- **EM/RF Interception:** Electro -Magnetic/ Radio Frequency interception to perform unauthorized interception of private communication.
- **Indiscretions by Personnel:** Lack of discretion of personnel could lead to unauthorized interception of private communication.
- **Media Scavenging:** It involves rummaging through disposed magnetic media for retrieving sensitive data that is left behind on it.
- **Intercept/ Alter:** Unauthorized people may intercept and alter the AMI data.
- **Repudiation:** People, including public authorities, may modify the AMI data and thus refuse to acknowledge an action that took place.
- **Masquerade:** It is a type of attack where the attacker pretends to be an authorized user of a system in order to gain access to it or to gain greater privileges than they are authorized for.
- **Bypassing Controls:** People may bypass security controls to get access to the confidential data and make unauthorized modifications.
- A**uthorization Violation:** People may violate the authorization of AMI system to perform unauthorized actions.
- **Physical Intrusion:** People may physically intrude into AMI system components like Smart Meter to perform unauthorized actions.
- **Man-in-the-Middle:** It is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection when in fact the entire conversation is controlled by the attacker.
- **Integrity Violations:** Integrity is violated when someone accidentally or with malicious intent modifies the AMI interaction data.
- **Theft:** Physical theft of the AMI components could lead to unauthorized actions being performed.

---

[24] Cyber Security Issues for Advanced Metering Infrastructure (AMI); F. M. Cleveland Senior Member IEEE, IEEE T&D Conference, April 2008

Advanced Metering Infrastructure Security Considerations; Raymond C. Parks; Assurance Technologies and Assessments, SANDIA REPORT, SAND2007-7327; Sandia National Laboratories

- **Replay:** It is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed.
- **Virus/Worms:** A computer virus is a computer program that can copy itself and infect a computer. A computer worm is a self-replicating computer program. It uses a network to send copies of itself to other nodes (computers on the network) and it may do so without any user intervention.
- **Trojan Horse:** It is a term used to describe malware that appears, to the user, to perform a desirable function but, in fact, facilitates unauthorized access to the user's computer system.
- **Trapdoor:** An undocumented entry point into a computer program, which is generally inserted by a programmer to allow discreet access to the program.
- **Service Spoofing:** It is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage.
- **Resource Exhaustion:** Hackers may use up all available facilities so no real work can be accomplished and thus AMI system resources become unavailable to the intended users.
- **Integrity Violations:** Integrity is violated when someone accidentally or with malicious intent modifies the AMI data and thus prevents intended users from using the AMI system resources.
- **Stolen/Altered:** The AMI data could be stolen or altered and that could lead to denial of action that took place or claim of an action that did not take place.
- **Repudiation:** People, including public authorities, may refuse to acknowledge an action that took place.
- **Insider Attack:** The insider attack would take advantage of access to systems at the opposite end of the AMI system from the customer endpoint. The systems that the insider may be able to access include the AMI head-end, the system from which it gets pricing information (either EMS or ICCP server to an ISO or generation entity), and the network infrastructure supporting both of those systems. Which cyber-effect an insider uses would depend upon their access to these systems.
- **Unauthorized Access from Customer Endpoint:** There is a potential for AMI to allow access to the bulk electric grid from the residential or small business customer endpoint. The adversary can suborn the customer endpoint, crack wireless communications between the AMI meter and other endpoint equipment, or crack wireless communications from the AMI meter to the local concentrator. These attacks will expose the head end equipment and systems to which the head end are connected. The exact details of this attack are greatly dependent on the implementation of AMI, particularly at the head end. Certain configurations would allow an attacker to affect the bulk electric grid.
- **Cheating Customer:** The customer at an endpoint would attack to achieve the goal of reduced cost of electric and/or natural gas use. They would use information freely

available from the AMI meter vendor or a standard associated with AMI meters to reset the meter and reprogram it to report false information. If the information is not freely available, the attacker would reverse-engineer a meter to develop a way to modify it. This is very similar to the many cable modem attacks that are openly available. Either the configuration settings from the utility or the actual firmware controlling the operation of the meter would be modified in this attack.

The following table summarizes the various security threats on AMI with respect to security goals and potential threat level.

Table 2-1: Security Threats on AMI With Respect To Security Goals

Security Issue	Description	Security Goal Compromised	Security Threat Level
Listening	Unauthorized people listening to the AMI communication. • Eavesdropping • Traffic Analysis • EM/RF Interception • Indiscretions by Personnel • Media Scavenging	Confidentiality	High
Modification	Unauthorized modification of the AMI data. • Intercept/ Alter • Repudiation	Integrity	High
Interactions	Interactions of AMI components with the environment could lead to unauthorized access to AMI communication information, modification of AMI data, denial of service to authorized users, and non-repudiation. • Masquerade • Bypassing Controls • Authorization Violation • Physical Intrusion • Man-in-the-Middle • Integrity Violations • Theft • Replay	Confidentiality Integrity Availability Accountability	High
Planted in System	Malicious code/components planted in the system could lead to unauthorized access to AMI communication information, modification of AMI data, denial of service to authorized users, and non-repudiation.	Confidentiality Integrity Availability Accountability	High

Security Issue	Description	Security Goal Compromised	Security Threat Level
	• Virus/Worms • Trojan Horse • Trapdoor • Service Spoofing		
Denial of Service	It is an attempt to make AMI system resources unavailable to its intended users. • Resource Exhaustion • Integrity Violations	Availability	High
After-the-Fact	Denial of action that took place or Claim of the action that did not take place is covered under this category. • Stolen/Altered • Repudiation	Accountability	Medium
Insider Attack	The insider attack would take advantage of access to systems at the opposite end of the AMI system from the customer endpoint.	Confidentiality Integrity Availability Accountability	Low to High
Unauthorized Access from Customer Endpoint	There is a potential for AMI to allow access to the bulk electric grid from the residential or small business customer endpoint	Confidentiality Integrity Availability Accountability	High
Cheating Customer	The customer at an endpoint would attack to achieve the goal of reduced cost of electric and/or natural gas use.	Confidentiality Integrity Availability Accountability	Low to High

2.4 Demand Response Security Issues

2.4.1 Introduction

When electricity demand is peak, particularly in summer, utilities and other electric Independent Systems Operators (ISOs) keep electric generators on-line in order to meet high demand. This solution wastes energy and increases air pollution.[25] If the demand is highest in

[25] California Energy Commission's Public Interest Energy Research Program, PIER Buildings Program, "Automated Demand Response Cuts Commercial Building Energy Use and Peak Demand, Technical Brief", Public Interest Energy Research Program ,2008[online]. Available: http://www.energy.ca.gov/2008publications/CEC-500-2008-086/CEC-500-2008-086-FS.PDF. [Accessed October 15, 2009]

most regions and exceeds available supplies, brownouts and blackouts can happen. As a result, the electricity grids are not reliable enough. Many utilities, government, and others have been developing Demand Response (DR) to manage growth in peak electricity demands, and to provide more reliable electricity grids and more economic energy. Demand Response is "…an action taken to reduce electricity demand in response to price, monetary incentives, or utility directives so as to maintain reliable electric services or avoid high electricity prices."[26] During the peak hours, demand response programs or tariffs lower the energy use in return for decreasing total system costs and electric loads. Demand Response can reduce energy consumption during peak time or based on events (of which the energy prices are high), such as congestion, supply-demand balance and/or market conditions that raise the energy supply costs. Demand Response Research Center (DRRC) has been putting efforts to develop, demonstrate and deploy activities related to a framework which can enable automated demand response. The development of Open Automated Demand Response (OpenADR or Open Auto-DR) has been carried out in order to improve optimization between electric supply and demand which can improve the reliability of electronic grid and lower the total cost of overall systems. This section will mainly focus on security issues in communications and interfaces between the entities in DR system and OpenADR. OpenADR is "a set of standard, continuous, open communication signals and systems provided over the Internet to allow facilities to automate their demand and response with no human in the loop."[27] This chapter does not intend to focus on the details of how the DR and OpenADR systems operate. It may address some of Demand Response systems, but the main focus is on the security issues in the DR and OpenADR systems.

2.4.2 Demand Response and Security Concerns

The primary focus on the Demand Response (DR) is to provide the customers with pricing information so that the customers or the energy-management and control system (EMCS) at the customer's sites may respond based on the demands for electricity and electricity prices during some period of time. For instance, the customer may decrease demand (or shed load) during higher priced time periods or increase demand (or shift load) during lower priced time periods. The pricing information could be real-time based, tariff-based or some combination. DR could be implemented in many different ways based on the type of pricing signals. The real-time pricing (RTP) requires computer-based response, while the fixed time-of-use pricing may be manually handled by the customer based upon the time periods and the pricing. Since the pricing information could be transmitted electronically or fixed for long period and could be

---

[26] U.S. Federal Energy Regulatory Commission (FERC), "Assessment of Demand Response and Advanced Metering", 2007[online]. Available: http://www.ferc.gov/legal/staff-reports/09-07-demand-response.pdf. [Accessed October 17, 2009]

[27] S. Kiliccote, M.A. Piette, J.H. Dudley, Lawrence Berkeley National Laboratory (LBNL); E. Koch and D. Hennage, Akuacom, "Open Automated Demand Response for Small Commercial Buildings", Lawrence Berkeley National Laboratory ,July 2009 [online]. Available: http://drrc.lbl.gov/pubs/lbnl-2195e.pdf. [Accessed October 16, 2009]

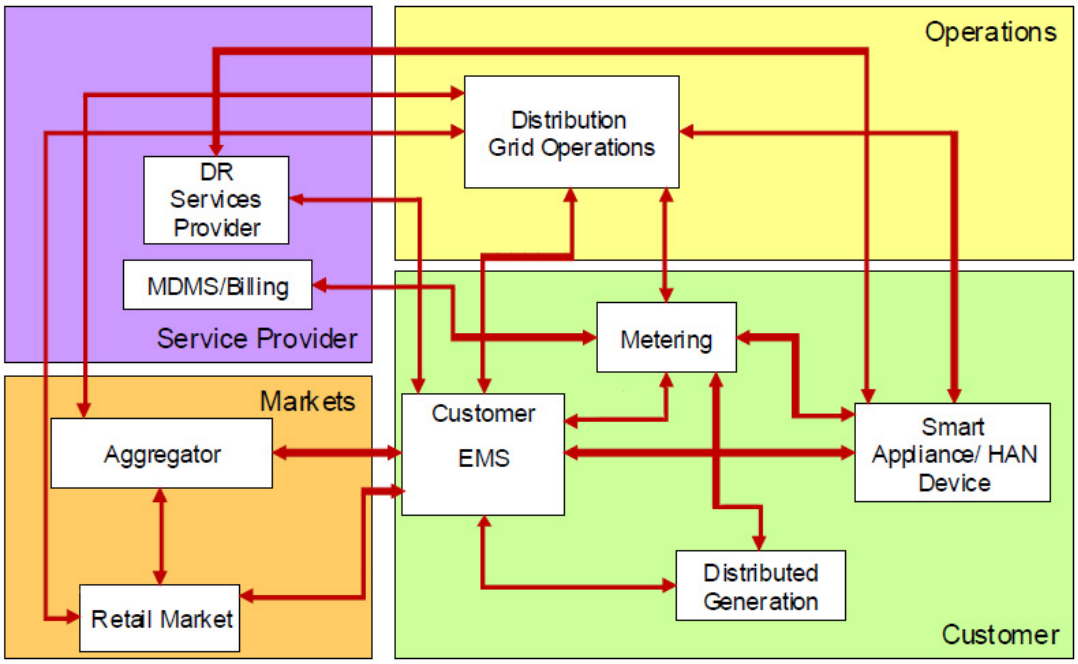
accessed by the participants of the DR program the customer's security and privacy should be addressed. Also, the integrity of the pricing signal is critical because if it can be manipulated, it could lead to financial impacts on the organization or customers. Thus, most of the DR functions in the smart grid, such as load shedding, time-of-use pricing (ToU), dynamic pricing, etc. require data integrity and/or confidentiality to maintain the reliability of the grid and prevent adversaries to manipulate the information in the system. Failure to provide integrity and/or confidentiality could result in the exposure of customer's information, unauthorized modification and manipulation of the information.

Security issues are explained below by first looking at interfaces of components that affect demand response. Next Auto Demand response systems are analyzed with respect to security.

Figure 2-2 shows the major components of Smart Grid that affect Smart Grid and their interactions.

Security Issues in Demand Response Interfaces

Figure 2-2: Demand Response Use Case



Source: Lawrence Berkeley National Laboratory/ Akuacom[28]

Shows the interfaces between each component (from NIST)

[28] A. Lee, T. Brewer, Computer Security Division, Information Technology Laboratory, National Institution of Standards and Technology (NIST) (Sept 2009). Smart Grid Cyber Strategy and Requirements (Draft NISTIR 7628). Available: http://csrc.nist.gov/publications/drafts/nistir-7628/draft-nistir-7628.pdf. [Accessed October 20, 2009]

2.4.2.1 Confidentiality

The information sent between each entity, such as control usage of the meter, pricing and metering usage and billing information, needs to be confidential and protected from unauthorized access to the information, such as eavesdropping attacks, since it can lead to the invasion of customer privacy and the leaking of the information to an adversary.

2.4.2.2 Authentication

The components in DR system, such as Home Area Network (HAN) Devices, Energy Management System (EMS), DR services provider and metering, must be authenticated in order to communicate with each other. If they fail to authenticate with the DR control services, they must not be able to connect or respond to the DR event signals in order to protect from the unauthorized devices to communicate with the DR system, such as hijacking of the meter connection.

2.4.2.3 Data Integrity

Unauthorized manipulation of demand information, control signals for the EMS to manage devices and control usage of the meter or smart meter by inducing an inappropriate response, such as turning on/off electrical devices at customer sections or shutting down DR operation, could directly decrease power reliability and quality of the grid and cause financial impacts as well as annoyance on customers. Also, manipulating the pricing signal could adversely impacts the customer and market sections financially.

2.4.2.4 Availability

Pricing and metering usage information need to be confidential, accurate and available all the time; otherwise, it would affect DR control behavior. The grid may not be able to response based on the signals and take a wrong action, leading to financial impacts on customers and markets. Real-time load use information transmitted between DR services provider and customer EMS needs to be available in the timely manner since it can affect the behavior of the grid. Legacy devices at end user and low bandwidth of communication channels may result in the loss of availability.

2.4.2.5 Accountability

Failure to hold account of the actions taken by communicating parties because of the invalid meter, EMS, or DR services provider information would result in the dispute between parties and decrease customer confidence.

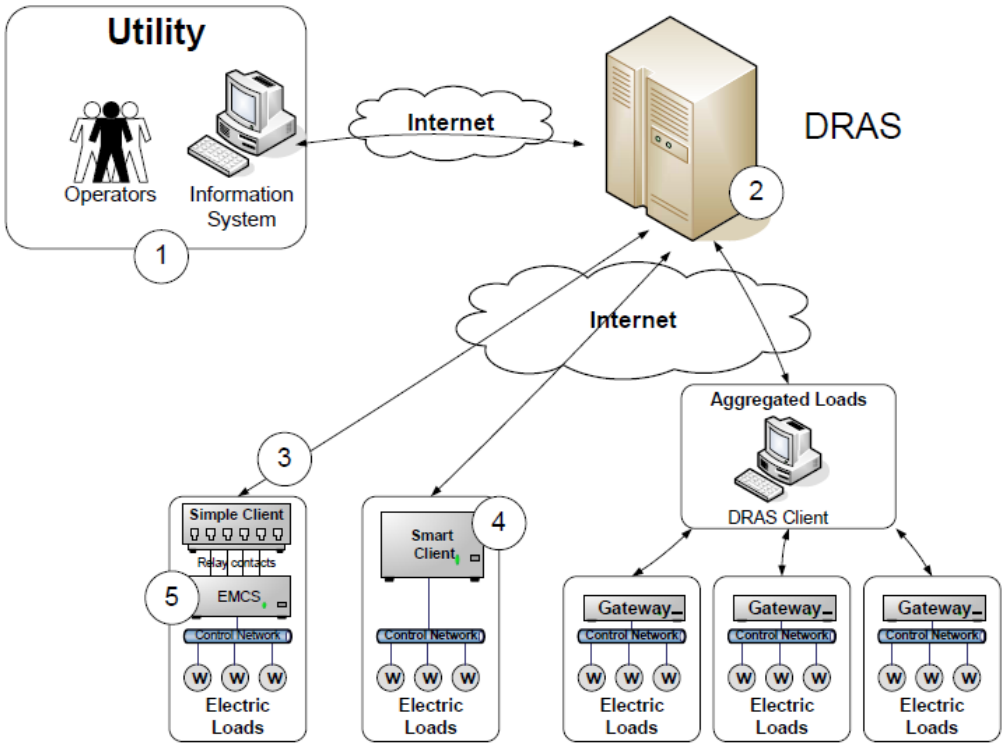
2.4.3 Open Automated Demand Response

OpenADR is a communications data model designed to interact with Demand Response signals by automated DR actions from Energy-Management and Control System (EMCS), which are pre-programmed, at electric consumer's sites. Internet-based electricity pricing and DR signals are used with pre-programmed control strategies to optimize energy use of a site or building with no manual intervention. OpenADR is used to exchange information between a utility or Independent System Operator (ISO) and the end-point users or customer systems.

2.4.3.1 Open Automated Demand Response Communications Infrastructure

OpenADR architecture depicted in Figure 2-3 consists of a Demand Response Automation Server (DRAS) and a DRAS Client. A server provides signals corresponding to DR events to notify customers and a client at the customer's site listens to the signals and automates signals to pre-programmed control systems (See Figure 2-3).

Figure 2-3: Generic Open Automated Demand Response Interface Architecture



Source: Lawrence Berkeley National Laboratory/ Akuacom[29]

[29] S. Kiliccote, M.A. Piette, J.H. Dudley, Lawrence Berkeley National Laboratory (LBNL); E. Koch and D. Hennage, Akuacom, "Open Automated Demand Response for Small Commercial Buildings", Lawrence Berkeley National Laboratory ,July 2009 [online]. Available: http://drrc.lbl.gov/pubs/lbnl-2195e.pdf. [Accessed October 16, 2009]

Information flow in the OpenADR architecture is in five steps, as follows:

1. The utility or ISO defines DR event and price signals that are sent to DRAS.
2. DR event and price services published on a DRAS.
3. DRAS clients, that can be a client and logic with integrated relay (CLIR) for a legacy control system or web service software for a sophisticated control system, request event information from the DRAS every minute.
4. Pre-programmed DR strategies determine action based on event and price.
5. EMCS carries out load shed based on DR events and strategies.

2.4.3.2 Demand Response Automation Server (DRAS)

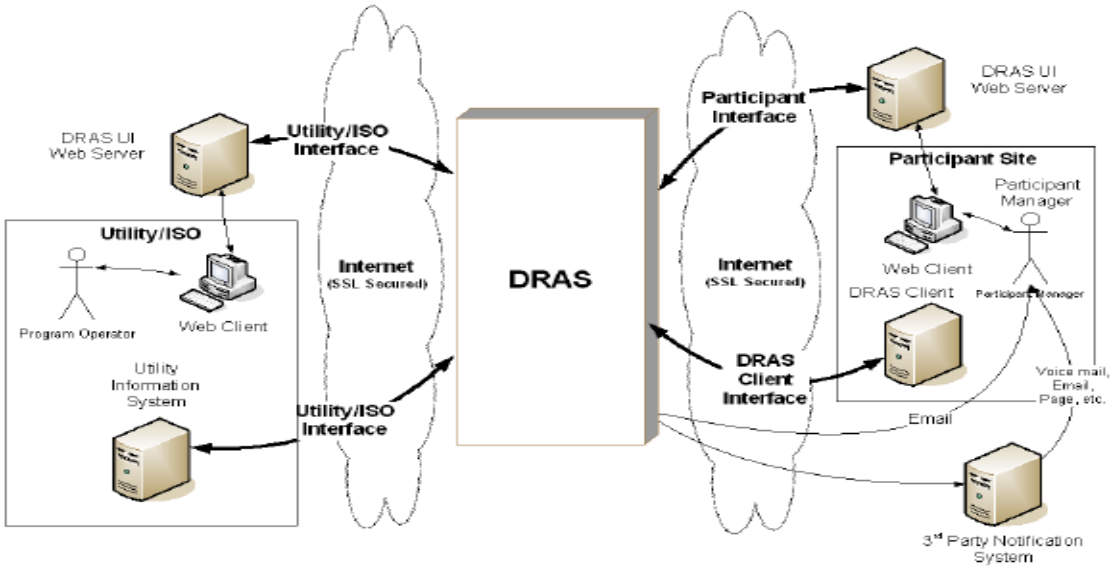
The DRAS is an infrastructure component in Automated Demand Response programs which are based on a client-server infrastructure. The automation server distributes and receives information among its entities, such as utilities and ISOs. The purpose of the DRAS is to automate dynamic pricing and reliable related messages and information received from utilities or ISOs to optimize the consumption of electricity during peak hours. The DRAS is an integrator between a Utility/ISO and DR participants. The major roles of DRAS are to notify the participants regarding real-time prices (RTP), DR events and DR related messages including dynamic pricing.

Figure 2-4 shows details of DRAS and its interface to utility and participant sites including the internet interface.

The DRAS interface can be implemented through WSDL or SOAP. XML can be used for the data model and the entities. The DRAS interface functions are divided into three groups as follows:

1. Utility and ISO Operator Interfaces
2. Participant Operator interfaces
3. DRAS Client Interfaces

Figure 2-4: DRAS Interfaces



Source: Lawrence Berkeley National Laboratory/Akuacom[30]

2.4.3.3 OpenADR and Security Concerns

Since the OpenADR system is based on the Internet communication, the information transmitted in each DRAS interface must be protected and prevented from any kinds of data manipulation, such as changing pricing information and DR events. The DRAS and DRAS clients need to be authenticated in order to communicate with each other. Also, access control to each entity in the OpenADR system is needed in order to protect from unauthorized access to the system. If the security goals are breached, potentially adverse impacts could occur, such as the excessive loads in the grid leading to blackouts and the large financial impacts on both the utility and participants in DR program.

This section is focusing on the security concerns on the information transmitted between the utility/ISO, DRAS and DRAS client. Table 5-1 below describes possible attacks and impacts that could happen if each security goal is compromised for each of the information transmitted in the OpenADR system. The information transmitted in the OpenADR is categorized into three groups based on the DRAS interfaces.

[30] M.A. Piette, G. Ghatikar, S. Kiliccote, E. Koch, D. Hennage, P. Palensky, and C. McParland, "Open Automated Demand Response Communications Specification", Demand Response Research Center, April 2009 [online]. Available: http://drrc.lbl.gov/openadr/pdf/cec-500-2009-063.pdf. [Accessed October 20, 2009]

Table 2-2: Possible Attacks Utility/ISO Operator Interfaces

Utility/ISO Operator Interfaces		
Purpose	**Information Transmitted**	**Security Concerns**
To initiate or update DR event information in DRAS	Program type, date & time of the event, date & time issued, geographic location, customer list (account numbers) and load shed event information.	**Confidentiality (L):** Eavesdropping on this formation is not of concern since the information may not be sent regularly. However, the information needs to be protected from unauthorized access. **Integrity (H):** Attacker modifies configuration data in the DRAS, such as DR program data, customer list and shed event information, affecting the DR program behavior. Attacker issues false or malicious DR events in DRAS, causing blackouts and instability of the grid. Also, this may lead to the financial impacts on customers. **Availability (L):** Failure in communication between utility and DRAS
To initiate bid request in DRAS	Program type, date & time of the event, date & time issued, geographic location, customer list (account numbers), request for a bid (RFB) issue date & time, RFB close time, price offered for load reduction per time block.	**Confidentiality (H):** Eavesdropping on this formation could result in the leaking of bidding and also pricing information to the attacker. **Integrity (H):** Unauthorized manipulation on this information could affect the bidding program behavior. Attacker issues false bidding information, causing the false behavior of the bidding program and the financial impacts on customer. **Availability (L):** Failure in communication between utility and DRAS**.**
To set accepted bids in DRAS	Participant list (account numbers), accept or reject, load reduction bids per time block (for verification)	**Confidentiality (H):** Eavesdropping on this formation could lead to the invasion of participant's privacy. **Integrity (H):** Attacker modifies participant list or load reduction per time block, accepted or rejected bid, causing instability of the grid and having financial impacts on participants. Attacker issues accepted/rejected bids to DRAS clients which may make an inappropriate response, such as increase the loads, according to the false accepted or rejected bids received. **Availability (L):** Failure in communication between utility and DRAS

Table 2-3: Possible Attacks and Impacts of DRAS Client Interfaces

DRAS Client Interfaces		
Purpose	**Information transmitted**	**Overall Impacts**
To send shed or event information to trigger the event client to shed or shift loads at participant sites, facilities or aggregator sites	Utility event information for smart DRAS clients, such as date & time of the event, date & time issued mode and pending signals. Mode and pending signals for simple clients. Event pending signals for simple clients.	**Confidentiality (H):** Attacker intercepts information sent between DRAS and DRAS client to gain knowledge of DR events, pricing information, customer information. Loss of confidentiality on this information can lead to the exposure of customer data, unauthorized modification of information, manipulation of information, malicious attacks, etc. causing the instability of grid and financial impacts on customers. **Integrity (H):** Attacker issues false/malicious DR events. Attacker may be able to turn on air conditioning or heater units in a large commercial building which can cause excessive loads to the gird and blackouts may take place, resulting in the instability of the grid and financial impacts on customers. Attacker may be able to shut down all air conditioning units which can cause annoyance and possible health concerns in some customers. Attacker issues false time synchronization, causing events to occur sooner or later than they normally would have. The signals need to be authenticated that they actually came from the DRAS. Inability to authenticate DRAS, DRAS client and Utility Information Service (UIS) can lead to a number of attacks, such as authentication sniffing, denial of service (DoS), man-in-the-middle attack, etc. Attacker captures an authentic signal, prevents the required reduction in load forcing utilities to take other measures such as buying energy at higher costs, and blackouts could occur. **Availability (H):** Attacker prevents the reduction of the load by disabling DRAS clients from receiving the incoming DR signals using denial of service attacks. Attacker floods the DRAS communications channel with non-DR related Internet traffic. Failure in communication between DRAS and DRAS clients.

DRAS Client Interfaces		
Purpose	**Information transmitted**	**Overall Impacts**
		Accountability (M): Participant denies receiving DR events. Participant denies receiving bidding information.
To send request for bid to participant or facility manager or aggregator	This information comes in the form of an email, phone call or page.	**Integrity (L):** An adversary may manually send an email, make a phone call or submit a page to the participant or facility manager so that the manager may respond to the adversary instead of to DRAS or the manager may take a wrong action in response to the bid request.
To notify the acceptance or rejection notification to the participant or facility manager or aggregator	This information comes in the form of an email, phone call or page.	**Integrity (L):** An adversary may manually send an email, make a phone call or submit a page to the participant or facility manager so that the manager may respond to the adversary instead of to DRAS or the manager may take a wrong action in response to the notification.

Table 2-4: Possible Attacks and Impacts of Participant Interfaces

Participant Interface		
Purpose	**Information transmitted**	**Overall Impacts**
To set, adjust or cancel standing bids in the DRAS.	Load reduction per time block (price and load amount)	**Confidentiality (M):** Attacker intercepts load reduction information sent from participant to the DRAS in order to gain knowledge of this information, causing the leak in the electricity usage of the customer. **Integrity (H):** Attacker submits bids for participants, causing the financial impacts on participants. **Availability (L):** Failure in communication between DRAS and DRAS client.
To send the system load status information to DRAS from DRAS clients.	Program identifier, facility or participant identifier, date & time of the event (shed or shift), shed data in kW/kWh, load reduction end uses (HVAC, lighting, etc.), event type (Day-Ahead or Day-Of)	**Confidentiality (H):** Eavesdropping on this formation could invade the customer privacy. **Integrity (H):** Unauthorized manipulation on this information could make DRAS not be able to record the actual response of the DRAS client to the DR events received. The DRAS may make an inappropriate response to the DR program according to the false system load status. This could lead to the unreliability of the grid.

Participant Interface		
Purpose	**Information transmitted**	**Overall Impacts**
		Availability (L): Failure in communication between DRAS and DRAS client.

2.4.4 Demand Response at Residential Sites and Security Issues

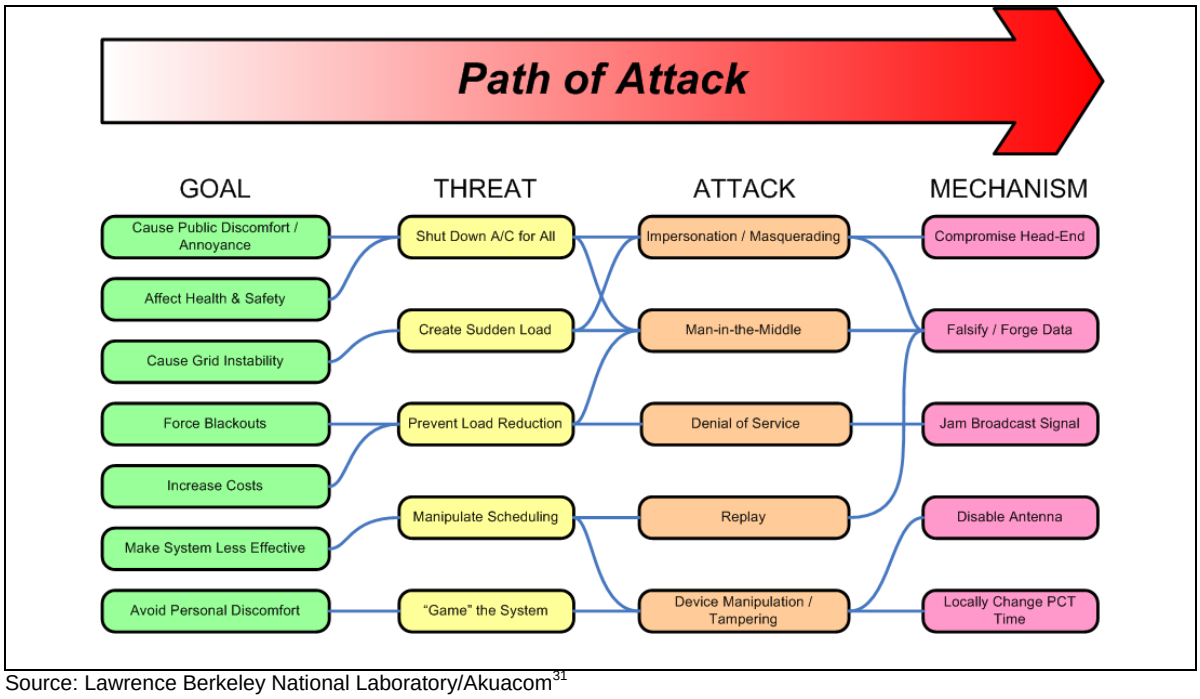
Demand response events arrive at the residential site from the utility to adjust the electricity price. During peak hours the price of the electricity rises; through demand response the customers can adjust their residential temperature on the basis of the demand response event received. During normal conditions, the broadcast messages consisting of price signals are sent, whereas during an emergency control signals are issued. The Programmable Communicating Thermostat (PCT) would be used in order to reduce the electric power at the residential site. Broadcast messages which will be sent out to the thermostat which causes the thermostat to update the power consumption. The PCT will be provided to the residential customers by the IOU's. The PCT will communicate with the utility through a meter. The connection is done through a wide area network. The PCT allows the customer to set the temperature for heating as well as cooling. Security issues such as confidentiality, integrity, availability and, non-repudiation come into effect for the PCT during the flow of events from the utility to the residential site. Integrity plays a crucial role in PCT. An attacker can cause annoyance, affect health and safety, grid instability by causing blackouts, and increase energy cost for the customer as some form of threats.

2.4.4.1 Possible Attacks in PCT

- An attacker may attempt to shut down the A/C, prevent the load reduction, and manipulate the scheduling of events received.
- An attacker tries to tamper with the incoming signals or PCT system. The attacker carries out the attacks by carrying out masquerading and man in the middle attack by shutting or turning down the A/C units in order to cause the grid instability.
- An attacker blocks the incoming broadcast signal by carrying out denial of service attack. Replay attacks can be carried out in order to manipulate the incoming demand response signal.
- An attacker could manipulate the system by disabling the PCT antenna or changing the PCT local time.

A summary of attack patterns in PCT is shown in Figure 2-5.

Figure 2-5: Path of Attack in PCT



Source: Lawrence Berkeley National Laboratory/Akuacom[31]

2.5 Customer Domain – Home Area Network, Gateway, and Neighborhood Area Network Security Issues

2.5.1 Introduction

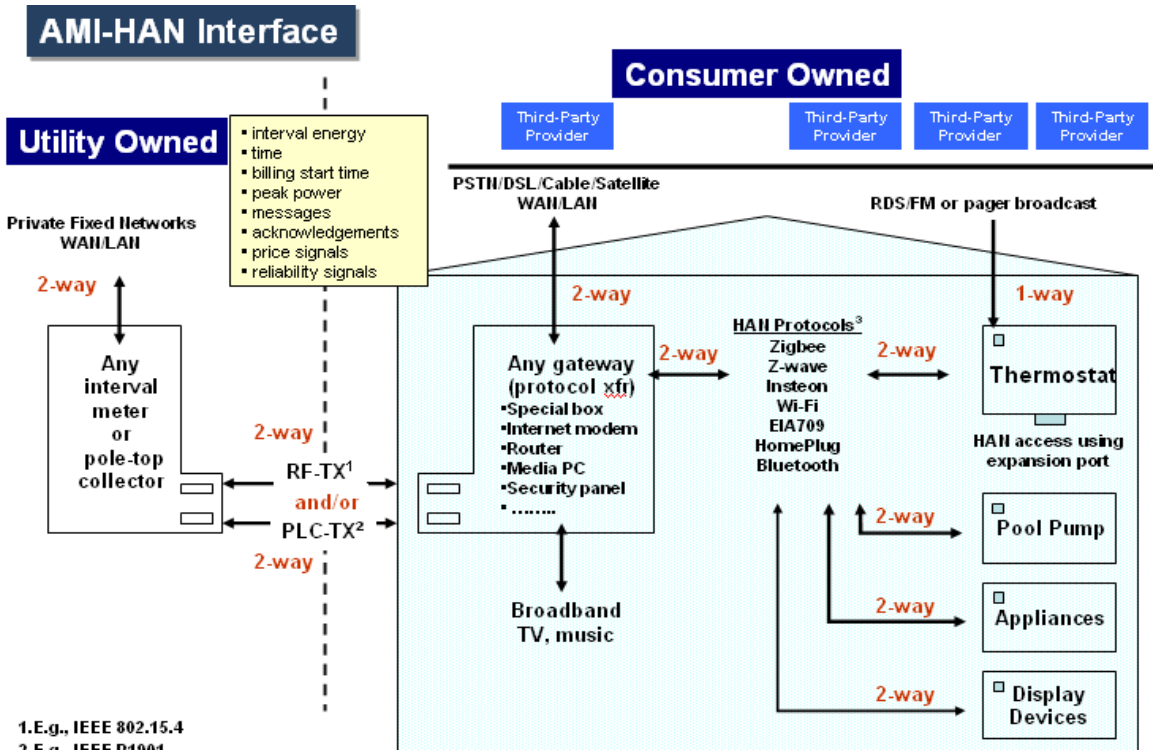
Actors in the Customer domain enable customers to manage their energy usage and generation. Some actors also provide control and information flow between the customer and the other domains. The boundaries of the customer domain are typically considered to be the utility meter. The customer domain is electrically connected to the distribution domain. It communicates with the Distribution, Operations, Market, and Service Provider domains. The reason why this section is subdivided into HAN, gateway and Neighborhood area network is that each actor contributes to making the customer interaction with the smart grid a possibility. Therefore we will handle each of the domains in the same order

Figure 2-6 depicts the entire customer domain with components such as Utility, AMI-HAN interface, Gateway and multiple HAN protocols which help connect various smart appliances in the Home area network. Along with HAN, gateway there exist WNAN as well which is depicted in the figure below as communication between smart meter and the utility. The two communication standards considered in this figure are Wireless Neighborhood Area Network (WNAN) and Local Area Network (LAN).

---

[31] E. W. Gunther, "Reference Design for Programmable Communicating Thermostats Compliant with Title 24-2008", March 2007 [online]. Available: http://drrc.lbl.gov/pct/docs/ReferenceDesignTitle24PC_rev15.doc. [Accessed October 22, 2009]

Figure 2-6: HAN/Gateway



Source: From the draft document on Residential Gateway Reference Design meeting held at UC Berkley

2.5.2 Home Area Network (HAN)

Smart Grid provides two-way communications between homeowners' premises and utility companies' back-end IT infrastructure. This is done by deploying Advanced Metering Infrastructure (AMI) systems that combine Home Area Networks (HANs) and Neighborhood Area Networks (NANs). A HAN typically connects home devices together whereas a NAN connects the home for the Utility Network. The key enabling technology for energy management products in the home are protocols such as ZigBee and Z-Wave, ultra-low power IEEE 802.15.4-based wireless networking standard that has emerged as the key to robust, reliable and secure HAN deployments. Although there are several other potential HAN Protocols, ZigBee is the only one discussed in detail, since it is the most popular open standard for HANs.

2.5.2.1 ZigBee

Following the standard OSI reference model, ZigBee's protocol stack is structured in layers. The physical and the media access layer are based on the 802.15.4 standard. The layers on top of these two layers are specific to Zigbee. They are the network layer, General Operation Framework (GOF) and the application layer. IEEE 802.15.4 is a standard which specifies the physical layer and media access control for low-rate wireless personal area networks. It focuses on low-cost, low-speed ubiquitous communication between devices (in contrast with other, more end user-oriented approaches, such as Wi-Fi). The emphasis is on very low cost

communication of nearby devices with little to no underlying infrastructure, so as to exploit this to lower power consumption.[32] It is the basis for ZigBee.

ZigBee makes it practical to embed wireless communications into virtually any home/building automation/metering product without the prohibitive cost and disruption of installing hard wiring. ZigBee allows individual devices to work for long periods of time (approximately 2+ years) on battery power.[33]

2.5.2.2 Z-Wave

Z-Wave is a wireless communications proprietary standard designed for home automation, specifically to remote control applications in residential and light commercial environments. The technology, which is developed by Zensys, uses a low-power RF radio embedded or retrofitted into home electronics devices and systems, such as lighting, home access control, entertainment systems and household appliances. Since it is a proprietary standard, not much information is available on Z-Wave.[34]

2.5.3 Gateway Component

Home Gateway (HG), also called Residential Gateway (RG) is a device that interconnects various home electronic devices to one another as well as connects these private home network devices to exterior public network. In the smart grid architecture the current assumption is that there is an identifiable unit performing the gateway function. But whether the gateway will be an independent functional unit or will it be a part of other smart grid component is an open possibility.

There are two implementation techniques for the gateway:

- The gateway is part of the PCT (Programmable Communicating Thermostat), one such example is the U-SNAP (Utility Smart Network Access Port).[35] This is a hardware solution to the interoperability issues between the native AMI network and the home area network. U-SNAP card brings a Serial interface between the module that communicates with the Utility AMI network and the HAN control unit.

---

[32] K. Stouffer, J. Falco, K. Scarfone, Guide to Industrial Control Systems (ICS) Security, National Institution of Standards and Technology (NIST), Sept 2008 [online]. Available: http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf

[33] A. Lee, T. Brewer, Computer Security Division, Information Technology Laboratory, National Institution of Standards and Technology (NIST), Smart Grid Cyber Strategy and Requirements, Draft NISTIR 7628, Sept 2009 [online]. Available: http://csrc.nist.gov/publications/drafts/nistir-7628/draft-nistir-7628.pdf

[34] E. W. Gunther, Reference Design for Programmable Communicating Thermostats Compliant with Title 24-2008 March 2007 [online]. Available: http://drrc.lbl.gov/pct/docs/ReferenceDesignTitle24PC_rev15.doc

[35] U-SNAP Alliance Industry White Paper ENABLING THE HOME AREA NETWORK MARKET. March 20, 2009

- A gateway as an individual component. This gateway implementation technique involves hardware component which integrates ZigBee based home automation system with an external IP based network. The gateway provides two functionalities:[36]
    - Data translation between the IP based network and the ZigBee network.
    - To provide a secure environment for processing command received from the external network.

The gateway consists of Wi-Fi module, a ZigBee Microcontroller and a power supply.

2.5.4 Wireless Neighborhood Area Network (WNAN)

The ubiquitous network requirements for Smart Grid are identified as follows: reliable, secure, power efficient, low latency, low cost, diverse path, scalable technology, ability to support burst, asynchronous upstream traffic to name a few. Wireless neighborhood area networks (WNAN) are a type of packet switched wireless mobile data networks. Wireless NANs are flexible packet switched networks whose geographical coverage area could be anywhere from the coverage of a Wireless Local Area Network (WLAN), to wireless metropolitan area network (WMAN), to Wireless Wide Area Network (WWAN). In Smart Grid, WNAN has a role to play in the HOME-to-HOME or HOME-to-GRID communication. The following are the communication protocols that are under consideration for wireless neighborhood area network for Smart Grid:

IEEE 802.11: IEEE 802.11 is a set of standards defined for the implementation of wireless local area network computer communication, which operates in the 2.4 GHz, 3 GHz and 5 GHz frequency bands. The 802.11b operates at 2.4 GHz with a data transfer rate in the range of 5 Mbits/s to 25 Mbits/s with a maximum outdoor range of 90 meters, while 802.11g operates at 2.4 GHz as well, with a data transfer rate in the range 22 Mbits/s to 128 Mbits/s with a maximum outdoor range of 90 meters.[37]

IEEE 802.15.4: 802.15.4 defines the physical and medium access control layers for low data-rate, short-range wireless communication. The operation is defined in both sub 1 GHz and 2.4 GHz frequency bands, supporting Direct Sequence Spread Spectrum signaling with a raw data throughput of 250 kbps and can transmit point to point, ranging anywhere from tens to hundreds of meters depending on the output power and receive sensitivity of the transceiver.[38]

IEEE 802.16: WiMax (Worldwide Interoperability for Microwave Access) that provides wireless transmission of data in variety of modes from a point to multi-point links. It is also called the Last Mile of Connectivity of Broadband wireless access with a range of around 50 km and a data

---

[36] Khusvinder Gill, Shuang-Hua Yang, Fang Yao, and Xin Lu A ZigBee-Based Home Automation System. Loughborough University, UK 2009.

[37] Wikipedia, IEEE 802.11: http://en.wikipedia.org/wiki/IEEE_802.11

[38] Naveen Shastry, David Wagner, Security Considerations for IEEE 802.15.4 Networks. UC Berkley. Year of Publication – 2004.

transfer rate of up to 70Mbps with the ability to support data, voice and video. It does not require LOS (Line Of Sight) and uses public key cryptography.[39]

2.5.5 Potential Security Issues/Risks

2.5.5.1 ZigBee40

1. Power Failures – Nonce [41](number used once) values are initialized to a standard value, thus making the nonce a known value.
2. Fast Denial-of-service Attack on AES-CTR (Advanced Encryption Standard CTR mode).
3. Acknowledges Forgery since the ACK frame returns only the DNS (Domain Name Server) value. If the attacker knows the DNS value he/she can send a false acknowledgement to the sender saying that the receiver has received the message when in fact it hasn't.
4. Weak Integrity Protection on AES-CTR.
5. Allows the use of Same Keys on multiple ACL (Access Control List) entries. Allows the use of Group Keys.

2.5.5.2 Z-Wave42

Unsecure connection while establishment of the network and distribution of the network key is taking place. Open to sniffer attacks.

Solution: The new device and the primary controller must be less than one meter apart for set-up. Once the new device has been included on the network database it can be placed anywhere within range of the network.

2.5.5.3 Gateway

Medium Access Control (MAC) address spoofing: When the U-SNAP card is plugged in for the first time it registers on the network. Since the network operates in an unlicensed frequency band any eavesdropper can listen to on-going traffic and spoof the MAC address, this MAC address the U-SNAP card uses as an ID to uniquely recognize a card. The second scenario occurs when pricing information is sent by the utility to the consumer, but the MAC address of the card has been spoofed. In this case the utility would be sending sensitive data to an unauthorized person which is breach of confidentiality of highest security level.[43]

---

[39] Wikipedia: WiMAX. http://en.wikipedia.org/wiki/WiMAX

[40] Matera: Security Issues on ZigBee Basilicata University, Italy, January 18, 2006

[41] A side input to the encryption algorithm.

[42] Wireless security - How safe is Z-wave? -Knight, M

[43] U-SNAP Alliance Industry White Paper ENABLING THE HOME AREA NETWORK MARKET. March 20, 2009.

Public Key Infrastructure security issues: The U-SNAP card uses Public Key infrastructure as a security feature. With the use of PKI emerges the problem of distribution of public keys and the added responsibility of choosing a certifying authority to sign the keys.[44] This issue is a problem for any system which uses PKI and is discussed further in chapter 9.

Virtual Home its security features and loopholes: In a virtual home, where in the gateway has added components such as virtual home, network coordinator and device data base. Every command which is received from the external network is checked for its authenticity by the network coordinator and the device data base in the virtual home environment. Once the command has been verified it's then implemented in the real home system. The security concerns with such a setup are as follows:[45]

- The gateway accepts commands even from a ZigBee based remote control and these commands are not verified in the virtual home environment. A malicious device emitting ZigBee signals could be interpreted as commands to the home environment.
- Since the gateway uses hardware components, device driver updates are needed. These updates should be done in a controlled manner; otherwise virtual home which is trusted for managing the security of the home area network will be compromised.

2.5.5.4 WNAN

IEEE 802.11[46]

- **Convenient Access**: Networks announce their existence with the aid of beacon frames which are also inviting threats. Software is used by "War Drivers" to log these appearances of beacon frames and find the locations using GPS.
- **Rouge Access Points**: One of the common security risks is with the rouge access points which are easy to setup and does not even require authorization.
- **MAC Spoofing**: The management frames are not authenticated in 802.11. Every frame has a source address. The attackers take advantage of the spoofed frame to redirect the traffic and corrupt the ARP tables.
- **Denial of Service Attacks**:
    - **Physical Attacks**: Simple devices that operate in 2.4 GHz frequency band like cordless phones that support 802.11b can be used to take the network offline. This is done by reducing the signal to noise ratio of the channel to an unusable range, by inducing noise into the network.

---

[44] John Linn, RSA Laboratories, Bedford, MA, USA Marc Branchaud, RSA Security Inc., Vancouver, BC, Canada. An Examination of Asserted PKI Issues and Pro-posed Alternatives. 2004.

[45] Khusvinder Gill, Shuang-Hua Yang, Fang Yao, and Xin Lu A ZigBee-Based Home Automation System. Loughborough University, UK 2009.

[46] Bob Fleck, Bruce Potter. 802.11 Security. O'Reilly Publications, December 2002, ISBN : 0-596-00290-4

- **Data-link Attacks**: For devices manufactured before 2003 with wired equivalent privacy (WEP) turned on, the attacker can perform DoS attacks by accessing the user information on the link layer. Data link attacks are difficult for post 2003 devices that support WPA2.

- **Network Attacks**: An attacker can flood ICMP packets to the gateway, thereby creating a difficult time for clients associated to the same AP to send and receive packet.
- **Man-in-the-Middle (MITM) Attacks**: There are two versions MITM attack. They are
  - Eavesdropping
  - Manipulating

Solution: Wi-Fi Protected Access (WPA) has an improved encryption algorithm called Temporal Key Integrity Protocol (TKIP) which uses unique key for every client and also uses longer keys that are rotated at configurable intervals. WPA also includes an encrypted message integrity check field in the packet to prevent denial-of-service and spoofing attacks.

IEEE 802.15.4[47]

1. **Confidentiality**: Encryption scheme must be used to prevent message recovery. The semantic security process is to encrypt the message twice to get two cipher texts. But if the same encryption process is used, then the semantic security is violated. The technique to prevent this violation is to uses a unique nonce† for each invocation of encryption process. The decryption uses this nonce at the receiver end, the nonce is sent clear in the same packet with the encrypted data and hence the security of encryption is not dependent on the nonce. The nonce is introduced to give some variations to the messages.

2. **Loss of ACL State**: Each ACL entry in the ACL table is used to store different keys and their associated nonce. There are chances of ACL table getting cleared when there is a power failure or when the device operates in a low powered state.
   - **Power Failure**: In case of power failures the ACL entries are cleared, however, the ACL table is repopulated by the software with appropriate keys. But, the issue is with the nonce states. All the nonce states are reset to a known value say 0 and there by reuse of nonce state incurred that compromises security.
   - **Low powered operation**: Again the issue is with how to retain the nonce states when the device enters the low powered state.

Possible Fix: Suitable fix to this problem could be saving and storing the nonce states in flash memories which incurs additional cost, power consumption and also is slow and energy inefficient.

---

[47] Naveen Shastry, David Wagner, Security Considerations for IEEE 802.15.4 Networks. UC Berkley. Year of Publication – 2004.

3. **Key Management Problems:** This problem arises due to the inability in the ACL tables to support different keying models.
    - **Group Keying**: There is no support for using the same key for multiple ACL entries. If attempts are made to create separate ACL entries for each node then the reuse of nonce state problem arises.
    - **Possible Fix**: Fix for this could be creating a single ACL entry for a particular key. Before sending, changing the destination address associated with that ACL entry for a message would suffice to fix this issue.
    - **Network Shared Keying:** The network cannot be protected from replay attacks when using a network wide shared key. In order to use the network shared keying model the application has to use the default ACL entry but a default ACL entry could be used only if there is no matching ACL entry.
4. **Confidentiality and Integrity Protection:** Researches have proven that unauthenticated encryption modes can introduce risks of protocol level vulnerabilities compromising not only integrity but also confidentiality. An example for this could be AES-CTR which uses counter mode without a MAC.
5. **Denial of Services**: As discussed previously, the replay attacks could cause the device to reject packets.
6. **No Acknowledgement Packets Integrity:** There is an option for the sender to request for an acknowledgement from the recipient for the sent packets. But there is no confidentiality or integrity provided for the acknowledgement packets thereby attracting the attacker to forge the acknowledgement packets.

IEEE 802.16[48]

- **Authentication:** The drawback with WiMax is that it does not have Base Station authentication which makes it prone to Man-in-the-middle attacks exposing subscribers to confidentiality and availability attacks. Since BS does not authenticate itself, the SSL cannot be protected from rouge BS.
- **Encryption:** 802.16e supports for Advanced Encryption Standard (AES) cipher providing strong confidentiality on user data. Again the drawback is with encryption not applied on the management frames thereby sufficing the attacker to gather information about the subscribers in the area and also about the network characteristics.
- **Availability:** Even though WiMax uses a licensed RF spectrum, attackers can use easily available gadgets to jam the network. This is an example for physical layer denial of service attacks whereas attackers can send legacy management frames to disconnect legitimate station, this is nothing but de-authenticate flood attacks.

[48] http://www.networkworld.com/columnists/2006/121106-wireless-security.html?page=1

- **Water Torture Attack:** This is a form of physical layer attack where in the attacker sends a series of frames to any node to drain the battery life of the victim node.

2.5.6 Comprehensive Security issues with HAN/ Gateway/ NAN

High -- High Security Risk
Medium – Medium Security Risk
Low – Low Security Risk

Table 2-5: HAN Security Issues

Component Involved	Threat Scenario Description	Security Threat Level
U-SNAP	MAC address spoofing Public Key Infrastructure security issues	High Confidentiality, Medium availability High Accountability High Integrity
ZigBee Gateway Module	Virtual Home its security features and loopholes	High Accountability High Integrity
ZigBee	Power Failures Fast Denial-Of-Service Attack on AES-CTR Acknowledges Forgery Weak Integrity Protection on AES-CTR Allows the use of Same Keys on multiple ACL entries	High Integrity High Availability High Accountability
IEEE 802.11	MAC Spoofing Denial of Service Attacks Man-in-the-Middle Attacks	High Confidentiality, High Accountability High Availability
IEEE 802.16	Authentication Encryption Availability Water Torture Attack	High Confidentiality, Medium Availability Medium Integrity
IEEE 802.15.4	Confidentiality Loss of ACL State Key Management Problems Encryption Denial of Services No Acknowledgement Packets Integrity	High Confidentiality High Integrity High Availability

2.6 Supervisory Control and Data Acquisition (SCADA) System Security Issues

2.6.1 Introduction

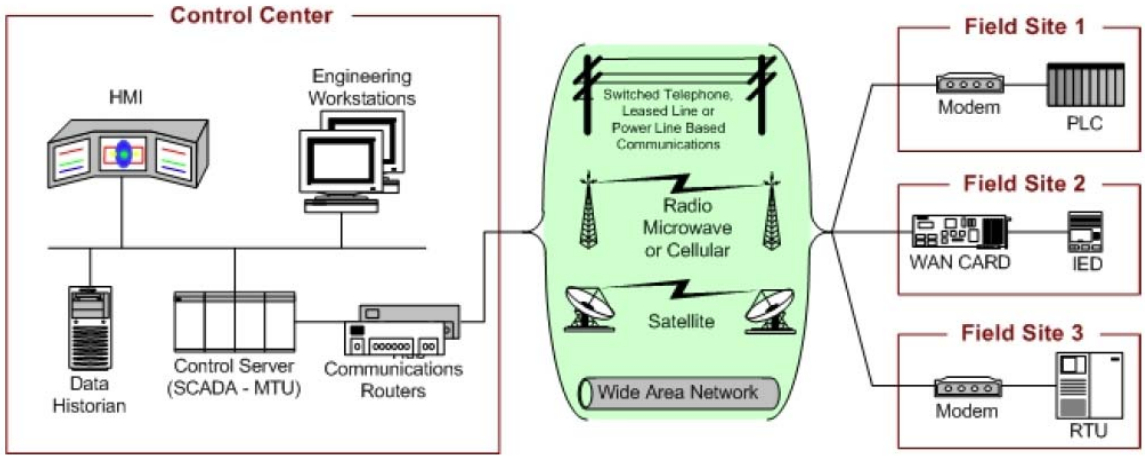
SCADA systems are widely deployed in Critical Infrastructure industries where they provide remote supervisory and control. In the Smart Grid SCADA systems are used in automation.

Despite the relevant importance of SCADA security, SCADA systems are reported to be vulnerable to electronic attacks. Taking into account the wide deployment of networking technologies in SCADA and a high connectivity of SCADA networks with other networks such as the corporate intranet or even the internet, SCADA systems are exposed to electronic attacks now more than ever.

This section discusses SCADA system security issues for the purpose of implementing an efficient defense of SCADA and Process Control Systems, in general, it is necessary to research on novel security approaches, implement them and carefully measure their suitability in terms of efficiency and overhead.

For instance, to monitor and control grid equipment such as transformers, customer equipment, generation and transmission system, etc. The general layout of a SCADA system is shown in figures 2-7 and figure 2-8 shows the SCADA architecture in more detail.

Figure 2-7: SCADA General Layout



Source: Guide to Industrial Control Systems (ICS) Security, National Institute of standards and technology

The figure above gives a general layout of a SCADA (Supervisory Control and Data Acquisition) system. SCADA is a collection of systems that measure, report, and change in real-time both local and geographically remote distributed processes. The fundamental components in the above figure are the control center usually computer-based, referred to as MTU (Master Terminal Unit), RTU (Remote Terminal Unit) or also called as field site, and the communication link between them. The MTU issues commands to distant facilities and gathers data from them, interacts with other systems in the corporate intranet for administrative purposes and interfaces

with human operators. In a SCADA system it is the MTU which has full control on distributed remote processes. An operator can interface with a MTU through an interface device consisting of a video display unit, a keyboard, etc. Control commands sent by a MTU to distant facilities are triggered by programs in that MTU which are executed either manually or through a programmable built-in scheduler.

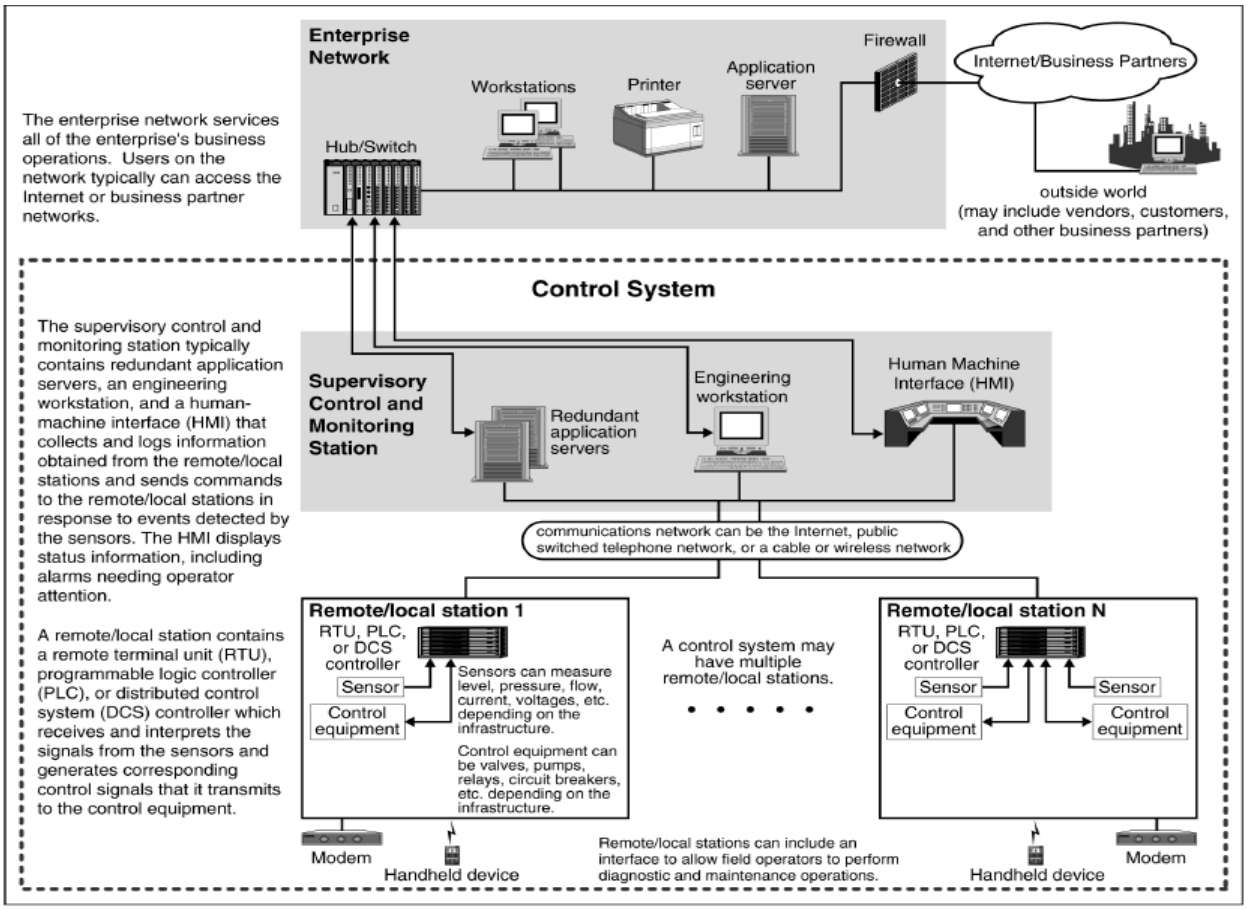
RTUs are generally based on microprocessors and are physically placed in remote locations. Their task consists of controlling and acquiring data from devices such as sensors, actuators, controllers, pulse generators, etc. An MTU communicates with one or more RTUs by sending requests for information that those RTUs gather from devices, or instructions to take an action such as open and close valves, turn switches on and off, etc. The communications between a MTU and RTUs follow a master-slave schema, in which the MTU is a master and RTUs are slaves, and only the MTU is allowed to initiate a transaction. [49]

The SCADA system is a control system which was originally designed to operate in an isolated environment. Today they are typically connected to the corporate network for business reasons. These Control Systems were also originally designed to be efficient rather than secure. Communication protocols (e.g. Distributed Network Protocol (DNP 3)) which allow remote control of the SCADA devices were designed with little security in mind. Impact of attacks on SCADA systems could be physical, economic, or societal.

The following sections discuss security issues in SCADA systems.

[49] National Institute of Standards and Technology, US department of Commerce (September 2008). Guide to Industrial Control Systems (ICS) Security (Special Publication 800-82 FINAL PUBLIC DRAFT). Keith Stouffer, Joe Falco, Karen Scarfone.

Figure 2-8: SCADA Architecture.50



Source: Critical Infrastructure Protection, Challenges in Securing Control Systems.

2.6.2 Security Issues in SCADA

2.6.2.1 Public Information Availability

Often, too much information about a utility company's corporate network is easily available through routine public queries. This information can be used to initiate a more focused attack against the network. Examples of this vulnerability are listed below:[51]

- Websites often provide data useful to network intruders about company structure, employee names, e-mail addresses, and even corporate network system names.
- Domain name service (DNS) servers permit "zone transfers" providing IP addresses, server names, and e-mail information.

---

[50] East, Samuel. Butts, Jonathan. Papa, Mauricio. And Shenoi, Sujeet. (2009). A taxonomy of attacks on the DNP3 Protocol. Critical Infrastructure Protection III, IFIP AICT 311, pp. 67–81, 2009. IFIP International Federation for Information Processing.

[51] Understanding SCADA System Security Vulnerabilities, Riptech

2.6.2.2 Platform Configuration Vulnerabilities

- OS and application security patches are not maintained.
- Inadequate Access controls. Poorly specified access controls can result in giving an SCADA user too many or too few privileges. The following exemplify each case: System configured with default access control settings gives operator administrative privileges, system improperly configured, results in an operator being unable to take corrective actions in an emergency situation.
- Password policies are needed to define when passwords must be used, how strong they must be, and how they must be maintained. Without a password policy, systems might not have appropriate password controls, making unauthorized access to systems more likely.[52]

2.6.2.3 Platform Software Vulnerabilities

- **Denial of service (DoS):** SCADA software could be vulnerable to DoS attacks, resulting in the prevention of authorized access to a system resource or delaying system operations and functions. They could proactively exploit software bugs and other vulnerabilities in various systems, either in the corporate network or the SCADA network, to gain unauthorized access to places such as control center networks, SCADA systems, interconnections, and access links. Cyber-attacks that are based on denial of service (DoS) mechanisms, and others that spread due to viruses and worms by causing a traffic avalanche in short durations, can potentially bring down systems and cause a disruption of services and are known as Flood-based Cyber Attack Types.
- **Intrusion detection/prevention software not installed:** Incidents can result in loss of system availability; the capture, modification, and deletion of data; and incorrect execution of control commands. IDS/IPS software may stop or prevent various types of attacks, including DoS attacks, and also identify attacked internal hosts, such as those infected with worms. IDS/IPS software must be tested prior to deployment to determine that it does not compromise normal operation of the SCADA.[53]
- **Malware protection software not installed, definitions not current, implemented without exhaustive testing:** Malicious software can result in performance degradation, loss of system availability, and the capture, modification, or deletion of data. Malware protection software, such as antivirus software, is needed to prevent systems from being infected by malicious software. Outdated malware protection software and definitions

---

[52], [54] National Institute of Standards and Technology, US department of Commerce (September 2008). Guide to Industrial Control Systems (ICS) Security (Special Publication 800-82 FINAL PUBLIC DRAFT). Keith Stouffer, Joe Falco, Karen Scarfone.

leave the system open to new malware threats. Malware protection software deployed without testing could impact normal operation of the SCADA.[54]

2.6.2.4 Network Configuration Vulnerabilities

The network architecture design is critical in offering the appropriate amount of segmentation between the Internet, the company's corporate network, and the SCADA network. Network architecture weaknesses can increase the risk that a compromise from the Internet could ultimately result in compromise of the SCADA system. Some common architectural weaknesses include the following:[55]

- Configuration of file transfer protocol (FTP), web, and e-mail servers sometimes inadvertently and unnecessarily provides internal corporate network access
- Network connections with corporate partners are not secured by firewall, IDS, or virtual private network (VPN) systems consistent with other networks
- Dial-up modem access is authorized unnecessarily and maintenance dial-ups often fail to implement corporate dial access policies
- Firewalls and other network access control mechanisms are not implemented internally, leaving little to no separation between different network segments

2.6.2.5 Network Perimeter Vulnerabilities[56]

Network Leak Vulnerabilities

- TCP/IP networks by their very nature promote open communications between systems and networks, unless network security measures are implemented. Improper network configuration often leads to inbound and outbound network leaks—between SCADA networks, corporate networks, business partners, regulators and outsourcers and even the Internet—which pose a significant threat to network reliability. Network leaks can allow worms, viruses or hackers direct visibility to vulnerable SCADA systems.

Insecure Connections Exacerbate Vulnerabilities

- Potential vulnerabilities in control systems are exacerbated by insecure connections. Organizations often leave access links—such as dial-up modems to equipment and control information—open for remote diagnostic SCADA, maintenance, and examination of system status. Such links may not be protected with authentication or encryption, which increases the risk that hackers could use these insecure connections to break into remotely controlled systems. Also, control systems often use wireless communications systems, which are especially vulnerable to attack, or leased lines that pass through commercial telecommunications facilities.

[54, 56, 57] National Institute of Standards and Technology, US department of Commerce (September 2008). Guide to Industrial Control Systems (ICS) Security (Special Publication 800-82 FINAL PUBLIC DRAFT). Keith Stouffer, Joe Falco, Karen Scarfone.

Firewalls nonexistent or improperly configured

- A lack of properly configured firewalls could permit unnecessary data to pass between networks, such as control and corporate networks. This could cause several problems, including allowing attacks and malware to spread between networks, making sensitive data susceptible to monitoring/eavesdropping on the other network, and providing individuals with unauthorized access to systems.

2.6.2.6 Network Communication (DNP 3) Vulnerabilities[57]

The SCADA systems are built using public or proprietary communication protocols which are used for communicating between an MTU and one or more RTUs. The SCADA protocols provide transmission specifications to interconnect substation computers, RTUs, IEDs, and the master station. The most common protocol is DNP3 (Distributed Network Protocol Version 3.3). It was developed to achieve interoperability among systems in the electric utility.

The following list presents features of DNP3 that provide benefits to the user:

- Open standard
- Interoperability between multi-vendor devices
- A protocol that is supported by a large and increasing number of equipment manufacturers
- Layered architecture conforming to IEC enhanced performance architecture model
- Optimized for reliable and efficient SCADA communications
- Supported by comprehensive implementation testing standards
- The ability to select from multiple vendors for future system expansion and modification

Here are some attacks which exploit the protocol specifications:

- Passive Network Reconnaissance: An attacker with the appropriate access captures and analyzes DNP3 messages. This attack provides the attacker with information about network topology, device functionality, memory addresses and other data.
- Baseline Response Replay: An attacker with knowledge of normal DNP3 traffic patterns simulates responses to the master while sending fabricated messages to outstation devices.
- Rogue Interloper: An attacker installs a "man-in-the-middle" device between the master and outstations that can read modify and fabricate DNP3 messages and/or network traffic.

---

[57] East, Samuel. Butts, Jonathan. Papa, Mauricio. And Shenoi, Sujeet. (2009). A taxonomy of attacks on the DNP3 Protocol. Critical Infrastructure Protection III, IFIP AICT 311, pp. 67–81, 2009. IFIP International Federation for Information Processing

- Length Overflow and DFC Flag Attack: These attacks either inserts an incorrect value in the Length field that affects message processing or sets the DFC flag, which causes an outstation device to appear busy to the master. These attacks can result in data corruption, unexpected actions and device crashes.
- Reset Function and unavailable function Attack: This attack sends a DNP3 message with Function Code 1 (reset user process) to the targeted outstation. The attack causes the targeted device to restart, rendering it unavailable for a period of time and possibly restoring it to an inconsistent state. Examples are interruption of an outstation and modification of an outstation. In unavailable function attack, the attacker sends a DNP3 message with Function Code 14 or 15, which indicates that a service is not functioning or is not implemented in an outstation device. The attack causes the master not to send requests to the targeted outstation because it assumes that the service is unavailable.
- Destination Address Alteration: By changing the destination address field, an attacker can reroute requests or replies to other devices causing unexpected results. An attacker can also use the broadcast address 0xFFFF to send erroneous requests to all the outstation devices; this attack is difficult to detect because (by default) no result messages are returned to a broadcast request.
- Fragmented Message Interruption: The FIR and FIN flags indicate the first and final frames of a fragmented message, respectively. When a message with the FIR flag arrives, all previously-received incomplete fragments are discarded. Inserting a message with the FIR flag set after the beginning of a transmission of a fragmented message causes the reassembly of a valid message to be disrupted. Inserting a message with the FIN flag set terminates message reassembly early, resulting in an error during the processing of the partially-completed message.
- Transport Sequence Modification: The Sequence field is used to ensure in-order delivery of fragmented messages. The sequence number increments with each fragment sent, so predicting the next value is trivial. An attacker who inserts fabricated messages into a sequence of fragments can inject any data and/or cause processing errors.
- Outstation Data Reset: This attack sends a DNP3 message with Function Code 15. The attack causes an outstation device to reinitialize data objects to values inconsistent with the state of the system. Examples of this attack are interruption and modification of an outstation.

Security Issues in SCADA and DNP 3 are summarized in Table 2-6.

Table 2-6: SCADA Security Issues

Security Issue	Description	Security Threat Levels
Public Information Availability	Information available through manuals, vendors, and through routine public queries.	Confidentiality
Policy and Procedure Vulnerabilities	Inadequate security policies, without the security architecture and design pose a threat. Lack of security audits,	Integrity

Security Issue	Description	Security Threat Levels
	disaster recovery plan etc.	
Platform Configuration Vulnerabilities	OS and application security patches are not maintained. Inadequate access control to systems, inadequate password policies.	Confidentiality, Integrity, Availability
Platform Software Vulnerabilities	Buffer Overflow. Denial of Service, Intrusion detection/prevention software not installed, malware protection not provided	Confidentiality, Integrity, Availability, Accountability
Network Configuration Vulnerabilities	Weak network security architecture, data flow control not applied	Availability, Integrity
Network Perimeter Vulnerabilities	Firewalls nonexistent or improperly configured, Insecure Connections Exacerbate Vulnerabilities, Network Leak Vulnerabilities	Confidentiality, Integrity, Accountability
Network Communication Vulnerabilities	Passive Network Reconnaissance Baseline Response Replay Rogue Interloper Length Overflow and DFC Flag Attack Reset Function and unavailable function Attack Destination Address Alteration Fragmented Message Interruption Transport Sequence Modification Outstation Data Reset Outstation Application Termination	Integrity Accountability Integrity Integrity, Confidentiality Availability Availability Integrity Integrity Integrity, Availability Availability

There is a recent security extension to DNP 3 but the researchers are not aware of their widespread implementation.

2.7 Plug In Electric Vehicles (PEV) Security Issues

2.7.1 Introduction

Despite the current high cost of maintaining electric vehicles, they are generally cheaper to operate over the long run because they reduce dependency on oil resources which have been fluctuating in price due to political instability of the nations that supply the natural oil. Electric vehicles also produce less greenhouse emissions than gas powered vehicles which will help reduce the effects of global warming.

Many technological and economical challenges come with the continued trend of PEVs becoming more prevalent. "In particular, battery technology (e.g., battery capacity and charge time) and the infrastructure (e.g., charge stations and grid), are essential prerequisites for a

massive deployment."[58] The Smart Grid will utilize Vehicle to Grid (V2G) which is one of the technological advances that will be used in making electric vehicles a viable mainstream option for prospective automobile customers. V2G will be a vital component for both the vehicle's owners and the energy providers because it will allow both parties to draw power from each other as needed. "Peak load leveling is a concept that allows V2G vehicles to provide power to help balance loads by "valley filling" (charging at night when demand is low) and "peak shaving" (sending power back to the grid when demand is high)."[59] V2G allows electric vehicle the capability to charge their batteries when energy demand is low while energy enables companies to draw power from the vehicles when there is a shortage of power. "Since most vehicles are parked an average of 95 percent of the time, their batteries could be used to let electricity flow from the car to the power lines and back, with a value to the utilities of up to $4,000 per year per car."[60] Seeing that V2G follows the concept of peak load leveling, power consumers and providers can help each other reduce cost and improve overall effectiveness of power distribution.

Even though there has been some progress in solutions for PEV technology, other security issues associated with the technology and the data it will use remain. Some potential for security issues related to PEVs include "Secure Payment and Privacy, Smart Metering, and the Critical Infrastructure and Physical Security."[61]

2.7.2 Privacy of Movement

PHEV will over load the smart grid when they are plugged-in for charging because the PHEVs move for place to place so the power requirements to the locations change. For example, there may be a city like Manhattan where more traffic flows in during peak office hours. If many PHEVs are plugged into the grid located at that point, at a time, it will overload the grid. To solve this problem the position of the PHEVs should be monitored. The constant monitoring of the PHEV location lends to privacy concerns to one's individual freedom. Additionally, if someone breaks into the monitoring system, they could get access to this information.

2.7.3 Secure Payment

A very important element to the smart grid is a payment system which works reliably and secure, and which protects both the end-user and the provider. There are good reasons to prefer electronic payment systems over cash payments, such as reduced revenue collection costs and reduce of losses; enhance customer satisfaction, improved services and operational efficiency as well as more flexible pricing strategies. One type of solution is to use credit cards. However

---

[58], [61] Paar, Christof, Andy Rupp, Kai Schramm, Andre Weimerskirch, and Wayne Burleson. Securing Green Cars: IT Security in Next-Generation Electric Vehicle Systems. Tech. Amherst: ECE Department, University of Massachusetts at Amherst.

[59], [62] Vehicle-to-grid. Vehicle-to-grid -Wikipedia, the free encyclopedia. Wikipedia, 2 Oct. 2009.

credit card systems do have problems as well. For example, transaction needs to be protected so that an individual's information is not revealed to third parties. Another approach would be to adopt Integrated Transportation Payment Systems (ITPS). Unfortunately, there are also examples of serious shortcomings of today's ITPS. Existing systems do not have mechanisms protecting their security and especially the privacy of their users. One problem is that some systems deploy cryptographically weak proprietary primitives. Currently e-cash protocols have been extensively studied. The study shows that it is possible to construct secure off-line payment that protect the anonymity of honest users but is nevertheless able to disclose their identities as soon as they try to cheat the system.

Potential attackers can be categorized as a small set of individuals, commercial companies, and government institutions. Typically regular individuals will attack the system to acquire private sensitive information in order to track individuals or attack the system because they are curious. On the other hand commercial companies will generate user profiles to increase their revenue. They will usually respect legal restrictions but they will also exploit legal loopholes. Finally, government institutions will have extensive power and they might even be able to define the legal environment. Therefore it is important to define a legal framework to account for companies and government institutions, and define technical solutions that account for individual attackers.

Privacy is a challenging problem, since it involves cryptographic theory, engineering, policy and sociology. In order to enable a deployment, adequate security and privacy mechanisms must be a requirement. To prevent malicious actions by attackers some form of IT security need to be introduced to systems. Such methods range from cryptographic mechanisms, to secure and privacy-preserving payment systems to a critical infrastructure interpretation of the electric car charging network. This should lead towards addressing the security problems.

2.7.4 Smart Metering

The owner of the PEV might want to report less electricity than what was actually delivered to the PEV's batteries, and the energy provider might want to charge for more energy than what was actually delivered. Even worse than these two would be a third party or middle man, such as a charging station, which would be able to cheat both the energy providers and the owners of the PEV. This can happen if care is not taken in securing the smart meter from tampering. There are best practices that can be applied to provide protection.

2.7.5 Critical Infrastructure & Physical Security

When PEV's becomes the norm, the link between the energy and transportation critical infrastructure will become tightly intertwined. Any malicious attack made against either one of these two critical infrastructures could potentially pose a threat to the security of these two infrastructures, specifically in the areas of traffic management, and payments for services rendered, pertaining to charging of a PEV. Since the link between these two critical infrastructures is in uncharted territory for both the energy and transportation critical infrastructure sectors, research will be needed to better understand the impacts of such a close relationship between the two sectors. If a malicious attack were to penetrate the defenses of either the energy or the transportation critical infrastructure, it would be devastation to both

critical infrastructures, monetarily and physically. Many businesses will not be able to operate without the ability to charge their vehicles. Traffic management will also become a problem, and can potentially lead to physical harm to individuals. Because of the severity of the problems that can be caused by a malicious attack, the Department of Defense should be an active participant in the security of the energy and transportations sectors of the critical infrastructures.

Physical Security of the equipment is also important to the security of PEV's. If an individual is allowed to take electricity without paying for it, most of the time that individual will take the opportunity. The Smart chargers will need to be secure enough so that a potential attacker cannot hack the smart charger for a PEV to provide their PEV with free electricity. There also might be attackers that are not only looking for free electricity; but also to obtain sensitive information from the smart charging of the current owner or previous owners of the smart charging device.

Sometimes attackers are not only looking to steal information or energy; but also looking to cause physical harm to the owner of the PEV. If a battery is overcharged there is a possibility that the battery will explode and cause physical harm to anyone in the vicinity of the explosion. The solution to such a problem should be multi-faceted. The manufactures of the battery should include circuitry to not allow over charging of their batteries and the smart meter should make sure that over charging of a battery is not allowed. Another place that an attacker can cause mischief is at a charging station for a PEV's, by either skewing the amount of energy purchased or by stealing credit card numbers via card skimmers. Particular care has to be taken when dealing with the physical security of the hardware that involves PEVs.

Successful integration of PEVs into the Smart Grid depends on overcoming the security challenges of "Secure Payment and Privacy, Smart Metering, and the Critical Infrastructure and Physical Security."[62]

2.7.6 Communication

The PHEVs might use cellular network for communication but there are vulnerabilities in this network that can be used as a means of getting access into the system, sending wrong information, attacking the system etc. The potential attacks that can be performed are, middle-man-attack, spoofing, etc.

[62] Paar, Christof, Andy Rupp, Kai Schramm, Andre Weimerskirch, and Wayne Burleson. Securing Green Cars: IT Security in Next-Generation Electric Vehicle Systems. Tech. Amherst: ECE Department, University of Massachusetts at Amherst.

2.8 Generic Security Issues of the Smart Grid

2.8.1 Introduction

These security issues are critical but they are not uniquely associated with a specific smart grid "logical" component. These issues could affect any smart grid component and refer to actual field cases. The researchers have not been able to verify these field cases with relevant California Utilities. When they do so they will document it in the future. Most of these issues addressed here can be found in NIST smart grid bottom-up security analysis of smart grid document as well as smart grid vulnerability list.

2.8.2 Authenticating and Authorizing Users (People) to Substation IEDs

The problem is how to authenticate and authorize users (maintenance personnel) to Intelligent Electronic Devices (IEDs) in substations in such a way that access is specific to a user, authentication information (e.g. password) is specific to each user (i.e. not shared between users), and control of authentication and authorization can be centrally managed across all IEDs in the substation and across all substations belonging to the utility and updated reasonably promptly to ensure only intended users can authenticate to intended devices and perform authorized functions.

Currently many substation IEDs have a notion of "role" but no notion of "user". Passwords are stored locally on the device and several different passwords allow different authorization levels. These role passwords are shared amongst all users of the device with the role in question, possibly including non-utility employees such as contractors and vendors. Furthermore, due to the number of devices, these passwords are often the same across all devices in the utility, and seldom changed.

Users may be utility employees, contractors, or vendor support engineers. Roles may include audit (read-only), user (read-write), administrator (add/remove/modify users), and security officer (change security parameters).

The device may be accessed locally in the sense that the user is physically present in the substation and accesses the IED from a front panel connection or wired network connection, or possibly wireless. The device may also be accessed remotely over a low-speed (dialup) or high-speed (network) connection from a different physical location.

A provision to ensure that necessary access is available in emergency situations may be important, even if it means bypassing normal access control, but with an audit trail.

2.8.3 Authenticating and Authorizing Maintenance Personnel to Smart Meters

Like IED equipment in substations, current smart meter deployments use passwords in meters that are not associated with users. Passwords are shared between users and the same password is typically used across the entire meter deployment. The security problem is similar to IEDs.

Access may be local through the optical port of a meter, or remote through the AMI infrastructure, or remote through the HAN gateway.

Meters generally have some sort of connectivity to an AMI head end, but this connectivity may be as slow as 1200 baud, or lower (e.g. some power line carrier devices have data rates measured in millibaud).

2.8.4 Authenticating and Authorizing Users (People) to Outdoor Field Equipment

Some newer pole-top and other outdoor field equipment supports 802.11 or Bluetooth for near-local user access from a maintenance truck. The problem is how to authenticate and authorize users (maintenance personnel) to such devices in such a way that access is specific to a user (person), authentication information (e.g. password) is specific to each user (not shared between users), and control of authentication and authorization can be centrally managed across the utility and updated reasonably promptly to ensure only intended users can authenticate to intended devices and perform authorized functions.

There are two problems. One is the security of the wireless channel. The second is how users are authenticated. The researchers suspect that just like IEDs and Smart Meters, there are passwords in the field device (e.g. pole top recloser) that will be the same across hundreds or thousands of devices and never changed, i.e. not specific to the user.

Access will usually be local via wired connections, or near-local via short-range radio, although some devices may support true remote access.

2.8.5 Authenticating and Authorizing Consumers to Meters

In case meters act as home area network gateways for providing energy information to consumers and/or control for demand response programs, if consumer are authenticated to meters, authorization and access levels need to be carefully considered, i.e., a consumer capable of supplying energy to the power grid may have different access requirements than one who does not.

2.8.6 Authenticating Meters to/from AMI Head Ends (Mutual Authentication)

It is important for a meter to authenticate any communication from an AMI head end, in order to ensure that an adversary cannot issue control commands to the meter, update firmware, etc. It is important for an AMI head end to authenticate the meter, since usage information retrieved from the meter will be used for billing, and commands must be assured of delivery to the correct meter.

2.8.7 Authenticating HAN Devices to/from HAN Gateways

Demand response HAN devices must be securely authenticated to the HAN gateway and vice versa. It is important for a HAN device to authenticate any demand-response or commands from the DR head end to order to prevent control by an adversary. Without such authentication, coordinated falsification of control commands across many HAN devices and/or at rapid rates could lead to grid stability problems. It is important that the DR head end authenticate the HAN device both to ensure that commands are delivered to the correct device, and that responses from that device are not forged.

Should a HAN device fail to authenticate, it will presumably be unable to respond to demand response signals. It should not be possible for a broad DOS attack to cause a large number of HAN devices to fail to authenticate and thereby not respond to a DR event.

2.8.8 Securing Serial SCADA Communications

Many substations and distribution communication systems still employ slow serial links for various purposes including SCADA communications with control centers and distribution field equipment. Furthermore, many of the serial protocols currently in use does not offer any mechanism to protect the integrity or confidentiality of messages, i.e., messages are transmitted in clear text form. Solutions that simply wrap a serial link message into protocols like SSL or IPSEC over PPP will suffer from the overhead imposed by such protocols (both in message payload size and computational requirements) and would unduly impact latency and bandwidth of communications on such connections. A solution is needed to address the security and bandwidth constraints of this environment.

2.8.9 Protection of Routing Protocols in AMI Layer 2/3 Networks

In the AMI space, there is increasing likelihood that mesh routing protocols will be used on wireless links. Wireless suffers from several well-known and often easily exploitable attacks partly due to the lack of control to the physical medium (the radio waves). Modern mechanisms like 802.11i have worked to close some of these holes for standard wireless deployments. However, wireless mesh technology potentially opens the door to some new attacks in the form of route injection, node impersonation, L2/L3/L4 traffic injection, traffic modification, etc. Most current on-demand and link-state routing mechanisms do not specify a scheme to protect the data or the routes the data takes, primarily because of the distributed nature of the system itself. They also generally lack schemes for authorizing and providing integrity protection for adjacencies in the routing system. Without routing security, attacks such as eavesdropping, impersonation, man-in-the-middle, and denial-of-service could be easily mounted on AMI traffic.

2.8.10 Key Management for Meters

Where meters contain cryptographic keys for authentication, encryption, or other cryptographic operations, a key management scheme must provide for adequate protection of cryptographic materials as well as sufficient key diversity. That is, a meter, collector, or other power system device should not be subject to a break-once break-everywhere scenario due to one shared secret being used across the entire infrastructure. Each device should have unique credentials and key material such that compromise of one device does not impact other deployed devices. The key management system must also support an appropriate lifecycle of periodic re-keying and revocation.

There are existing cases of large deployed meter bases using the same symmetric key across all meters, and even in different States. In order to share network services, adjacent utilities may even share and deploy that key information throughout both utility AMI networks. Compromising a meter in one network could compromise all meters and collectors in both networks.

2.8.11 Insecure Firmware Updates

The ability to perform firmware updates on meters in the field allows for the evolution of applications and the introduction of patches without expensive physical visits to equipment. However, it is critical to assure that firmware update mechanisms are not used to install malware. Best practices exist to deal with these issues.

2.8.12 Side Channel Attacks on Smart Grid Field Equipment

These attacks are based on physical accessibility (Substation, Pole-Top, Smart Meters, Collectors, etc.). A side-channel attack is based on information gained from the physical implementation of a cryptosystem. Tempest attacks similarly can extract data by analysis of various types of electromagnetic radiation emitted by a CPU, display, keyboard, etc. Tempest attacks are nearly impossible to detect. Syringe attacks use a syringe needle as a probe to tap extremely fine wire traces on printed circuit boards.

Smart grid devices that are deployed in the field, such as substation equipment, pole-top equipment, smart meters and collectors, and in-home devices, are at risk of side channel attacks due to their accessibility. Extraction of encryption keys by side channel attacks from smart grid equipment could lead to compromise of usage information, personal information, passwords, etc. Extraction of authentication keys by side channel attacks could allow an attacker to impersonate smart grid devices and/or personnel, and potentially gain administrative access to smart grid systems.

2.8.13 Key Management and Public Key Infrastructure (PKI)

Key management for Smart Grid devices that contain symmetric or asymmetric long-lived keys is essential. Standard PKI may not be appropriate since many devices will not have connectivity to key servers, certificate authorities, OCSP servers, etc. The scale of the systems involved and their distribution is unprecedented, as it will involve millions of devices. There will also be issues of cross-certification across different domains and checking for validity of certificates within the context of this unprecedented scale.

2.8.14 Patch Management

Specific devices such as IEDs, PLCs, Smart Meters, etc. will be deployed in a variety of environments and critical systems. Their accessibility for software upgrades or patches maybe a complex activity to undertake because of how distributed and isolated equipment can be. Also there are many unforeseen consequences that can arise from changing firmware in a device that is part of a larger engineered system. Control systems require considerable testing and qualification to maintain reliability factors.

The patch, test and deploy lifecycle is fundamentally different in the electrical sector. It can take a year or more (for good reason) to go through a qualification of a patch or upgrade. Thus there are unique challenges to be addressed in how security upgrades to firmware needs to be managed.

CHAPTER 3:
Best Practices for Handling Smart Grid Cyber Security

3.1 IT Best Practices for Smart Grid Cyber Security

3.1.1 Introduction

This chapter is about information security best practices that can be used to deal with smart grid threats, vulnerabilities and risks. That is, it covers mitigation and countermeasures to address those vulnerabilities. Unless otherwise stated the terms mitigation, countermeasure and best practices are used interchangeably in this chapter.

As mentioned above, this chapter is one part of a series of research tasks specified in a statement of work for the California Energy Commission as follows:

1. Identify the potential issues affecting the confidentiality, integrity, and availability of information flow in the Smart Grid system. For instance, hacker/terrorist use of malicious software to perform denial of service attacks on critical infrastructure such as the Smart Grid will be examined. Group the issues with respect to confidentiality, integrity, and availability.
2. Investigate which information security best practice(s) apply to smart grid and to what extent can they be applied. Best practices such as use of firewalls for perimeter defense, intrusion detection, incident response handing, defense in depth, etc. are well known in the information security arena. These best practices are intended to mitigate actions that violate confidentiality, integrity, and availability of the information flow in the smart grid.
3. Explore possible cyber security R&D issues that should be addressed in Smart Grid. Some of these could involve wireless sensors, wireless communication systems, monitoring, and incident response systems.
4. Identify and recommend which potential R&D efforts should and should not be confidential.
5. Identify technical and non-technical solutions to ensure the privacy of end user information. Because Smart Grid systems will contain end user information, privacy is critical.

This chapter is about the second task listed above.

Best practices for securing information systems can be found in a number of standards including NIST (NIST pub 800-14), ISO 27002, RFC 2196, etc. In the area of Smart Grid some best practices can be found in NERC CIP 002-009. A summary of some of these standards can be found in Wikipedia.[63]

[63] Wikipedia: Cyber Security Standards. http://en.wikipedia.org/wiki/Cyber_security_standards.

The intent of the best practices is to limit successful exploitation of vulnerabilities in a system because no system can be 100% secure. Although most of the best practices for securing IT systems can be applied to the Smart Grid, there are potential problems, most of which are discussed in the NIST Bottom up Cyber Security document.[64] In the following summary of Information Security Best Practices (not necessarily in priority order) some of the problems are mentioned as needed. For each best practice mentioned, comments are made as to what extent the security best practice can be applied to the smart grid. Some of these problems might require further research. This is stated where necessary.

3.1.2 General Best Practices for Securing IT Systems

3.1.2.1 Information Security Policy

Information security policy specifies high level plans including establishment of Information security officer, operational security procedures such as user and data authentication, backup policies etc. There is also an implementation guide which describes how the information security plans will be implemented. Enforcement and auditing, including penalties for violation, makes sure that security policies, plans, and implementation, are handled correctly. In the smart grid, these policy documents can be created in a straight forward manner and submitted to upper management for approval.

3.1.2.2 Software Updates and Patches

Software updates and patches are needed because software is usually not 100% secure. Attackers are finding new ways to exploit systems. Software to defend against new exploits must be used to update systems. Vendor patches and antivirus must be used to close the security holes. If patches and updates are not done, vulnerabilities are exponentially increased. Patch management procedures and frequency of the updates must be documented.

Although this can be done in the smart grid there are problems. For instance specific devices such as IEDs, PLCs, Smart Meters, etc. will be deployed in a variety of environments and critical systems in the smart grid. Their accessibility for software upgrades or patches maybe a complex activity since the equipment is typically distributed and isolated. Additionally, the patch, test and deploy lifecycle is fundamentally different in the electrical sector. It can take a year or more to go through a qualification of a patch or upgrade. Because deployment of a security upgrade or patch is unlikely to be as rapid as in the IT industry there needs to be a process whereby the risk and impact of vulnerability can be determined in order to prioritize upgrades. Also a security infrastructure needs to be in place that can mitigate possible threats until the upgrade can be qualified and deployed so that the reliability of the system can be maintained.

Another issue is to ensure that the updates are done securely since they will likely be done online to prevent expensive physical visits to equipment. Therefore, it is critical to assure that firmware update mechanisms are not used to install malware. This can be done with a combination of strong authentication/authorization mechanisms for the person performing

[64] NIST: http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CSCTGBottomUp

updates, integrity mechanism to ensure that the firmware is secure, and remote attestation mechanisms to ensure that the correct version is being updated. Finally, there should be ways to detect tampering.

3.1.2.3 Physical Security

Having rules about who can physically access an asset (information or equipment) and how they gain entry can decrease the likelihood that an unauthorized individual is present to access information. Additionally, policy documents should discuss how a physical asset is stored and destroyed.

In the Smart grid infrastructure this best practice can be applied to the business, and some operational entities. On the other hand, in the case of smart meters for instance it is difficult to maintain physical security so one has to assume that an attacker can gain physical access to it. This means that the meter should be made tamper-resistant or tamper-evident. Ability to make a cost-effective tamper-resistant meter is not an easy problem.

3.1.2.4 Data Classification and Retention

Data classification refers to classifying data according their security (confidentiality, integrity, or availability) level. Retention refers to how long data is kept before destroyed. The purpose of this best practice is to reduce an organization's liability by classifying exactly what type of data is needed and how long it is needed. For example there have been cases where a breach occurred and sensitive data (credit card number) which had no business need of being kept was stolen.

In the smart grid this principle can be used in the business side of the smart grid in a straight forward manner. However in the operational and distribution side it could be a problem because there could be energy data about a customer that could reside in a meter, meter data management system, or AMI headend. Meter data especially is unattended. Clearly, there are privacy issues that apply. Another issue is what happens to meter data when a house changes hands. The NIST smart grid privacy group is currently looking at these problems.

3.1.2.5 Employee Awareness, Training, and Education

How well informed employees are about security issues can help to identify or prevent a security incident. The old adage 'security is based on the weakest link' makes this imperative. In many respects each employee is a member of an organization's security army. Training is needed, and expectations should be set appropriately and communicated clearly in a policy. There are different levels of training. There is awareness training and technical training depending on employee background and job classification.

In the smart grid this best practice can be applied in a straightforward manner.

3.1.2.6 Incident Response

Incident response is important because a breach is inevitable since no system can be 100% secure. Incident response procedures should be developed so that it is used in the event of an incident. Incident response includes disaster-recovery and business-continuity plans. To response to an incident the incident must be detected. In traditional IT systems incidents can be

detected with firewalls and/or intrusion detection systems that use a database of past attack signatures. Machine level intrusion typically involves using hashes of known system software.

In the smart grid these methods can be used in the business side of systems. In the operation, distribution, and customer level, the methods mentioned above cannot be applied directly. For instance a smart meter will typically not have enough memory or computational power to store the database of attack signatures. Additionally, because of the millions of devices involved there could be too much network traffic if the devices have to access an external database. Finally, because the smart grid is a control system as well as critical infrastructure it is beneficial to employ real time intrusion detection. This is different from classical IT systems where intrusion is detected and the response is done after the fact. In the smart grid one wants to be able to respond to incidents without shutting systems down. Further research is needed in these areas.

3.1.2.7 Supply Chain Management

Security of a system is only as strong as the weakest link, and when an organization works with third-party providers their information security downfall can become their issue. Therefore, the organization should make sure to document for instance, which vendors receive confidential information and how this information is treated when in the custody of the vendor. The lack of strict vendor guidelines could increase the risk of releasing customers' private information.

In the smart grid this principle can be used in a straightforward manner in both business systems and customer domain to handle confidentiality. Another area where this principle is applicable is where integrity is managed in the supply chain. For instance, if a utility purchases a smart meter from a vendor, how does the utility know that the firmware is free of malware (perhaps inserted by a disgruntled employee), or that it cannot be exploited by an attacker's malware? This problem can be handled by documented agreement, review of vendor design and manufacturing processes, thorough testing of the meter through vulnerability assessment, vendor reputation, etc.

3.1.2.8 Password Requirements and Guidelines

Employees dread having another password to remember. The more complicated requirements are made to ensure password security, the more employees decide to write them down and consequently expose them to others. It is good to establish a strong password policy but stay within reason for employees. Sometimes, additional training on teaching employees how to choose good passwords and recognition of social engineering techniques attackers use to obtain passwords will help. Additionally, training employees as to why the policy is the way it is can go a long towards gaining employee acceptance.

3.1.3 System Life-Cycle Management

System Life-Cycle Management in systems engineering and software engineering, is the process of creating or altering systems, and the models and methodologies that people use to develop these systems. There are five basic stages in a 'System Development Life Cycle'. This cycle refers to the entire path that needs to be followed while developing a product, ensuring maximum success of the product and a minimum chance of a failure. Such a life cycle has also been introduced in the security domain, it is known as the "Security Design Life Cycle (SDLC)".

Figure 3-1 shows a typical system development life cycle. The five stages of SDLC are described below.

Figure 3-1: Conceptual view of SDLC[65]

Stage 1: Initiation:
During this first phase of the development life cycle, security considerations are key to diligent and early integration, thereby ensuring that threats, requirements, and potential constraints in functionality and integration are considered. Early planning and awareness will result in cost and timesaving through proper risk management planning. Security discussions should be performed as part of the development project to ensure solid understandings among project personnel of business decisions and their risk implications to the overall development project.

Three essential steps to be followed in this Initiation phase are summarized in Table 3-1, Table 3-2 and Table 3-3.

[65] NIST Document 800-64: http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf

Three essential steps to be followed in this Initiation phase are summarized in Table 3-1, Table 3-2 and Table 3-3.

1. Initiate Security Planning;

Table 3-1: Initiate Security Planning

Description	Security planning should begin in the initiation phase by: Identifying key security roles for the system development; Identifying sources of security requirements, such as relevant laws, regulations, and standards; Ensuring all key stakeholders have a common understanding, including security implications, considerations, and requirements; and Outlining initial thoughts on key security milestones including time frames or development triggers that signal a security step is approaching. This early involvement will enable the developers to plan security requirements and associated constraints into the project. It also reminds project leaders that many decisions being made have security implications that should be weighed appropriately, as the project continues.
Expected Outputs	Supporting documents (slides, meeting minutes, etc.) Common understanding of security expectations. Initial schedule of security activities or decisions.
Synchronization	A series of milestones or security meetings should be planned to discuss each of the security considerations throughout the system development.

2. Assess the Impact of Privacy;

Table 3-2: Assess the Impact of Privacy

Description	When developing a new system, it is important to directly consider if the system will transmit, store, or create information that may be considered privacy information. This typically is identified during the security categorization process when identifying information types. Once identified as a system under development that will likely handle privacy information, the system owner should work towards identifying and implementing proper safeguards and security controls, including processes to address privacy information incident handling and reporting requirements.

Expected Outputs	Privacy Impact Assessment providing details on where and to what degree privacy information is collected, stored, or created within the system.
Synchronization	Should continue to be reviewed and updated as major decisions occur or system purpose and scope change significantly.

3. Ensure Use of Secure Information System Development Processes;

Table 3-3: Ensure Use of Secure Information System Development Processes

Description	Primary responsibility for application security, during early phases, lies in the hands of the development team who has the most in-depth understanding of the detailed workings of the application and ability to identify security defects in functional behavior and business process logic. They are the first level of defense and opportunity to build in security. It is important that their role not be assumed or diminished. Communicating and providing expectations is key to planning and enabling an environment that protects down to the code level. As a team, system developers and security representatives should agree on what steps can and should be taken to ensure valuable and cost-effective contributions to a secure development environment.
Expected Outputs	Plans for development phase security training. Planned quality assurance techniques, deliverables, and milestones. Development and coding standards including development environment.
Synchronization	Lessons learned from completed products and security testing should be evaluated for appropriateness in adjusting development processes and standards to prevent embedding weaknesses.

Stage 2: Description:
This section addresses security considerations unique to the second SDLC phase. Key security activities for this phase include:

- Conduct the risk assessment and use the results to supplement the baseline security controls;
- Analyze security requirements;
- Perform functional and security testing;
- Prepare initial documents for system certification and accreditation; and
- Design security architecture.

Although this section presents the information security components in a sequential top-down manner, the order of completion is not necessarily fixed. Security analysis of complex systems will need to be iterated until consistency and completeness is achieved.

There are five major steps to be followed to fulfill the requirements in this phase; the tables 3-4 to 3-8 give an over view about the steps in this stage.

There are five major steps to be followed to fulfill the requirements in this phase; the tables 3-4 to 3-8 give an over view about the steps in this stage.

1. Assess the Risks to the System:

Table 3-4: Assess the Risks to the System

Description	The purpose of a risk assessment is to evaluate current knowledge of the system's design, stated requirements, and minimal security requirements derived from the security categorization process to determine their effectiveness to mitigate anticipated risks. Results should show that specified security controls provide appropriate protections or highlight areas where further planning is needed. To be successful, participation is needed from people who are knowledgeable in the disciplines within the system domain. The security risk assessment should be conducted before the approval of design specifications as it may result in additional specifications or provide further justification for specifications.
Expected Outputs	A refined risk assessment based on a more mature system design that more accurately reflects the potential risk to the system, known weaknesses in the design, identified project constraints, and known threats to both business and IT components. In addition, previous requirements are now transitioning into system specific controls.

Synchronization	Since this risk assessment is completed at a more mature stage of system development, there may be a need to revisit previously completed security steps, such as BIA or Security Categorization. Development rarely goes as planned, and requirements have a way of changing.

2. Select and Document Security Controls:

Table 3-5: Select and Document Security Controls

Description	The selection of security controls consists of three activities: the selection of baseline security controls (including common security controls); the application of security control tailoring guidance to adjust the initial security control baseline; and the supplementation of the tailored baseline with additional controls based on an assessment of risk and local conditions. An organization-wide view is essential in the security control selection process to ensure that adequate risk mitigation is achieved for all mission/business processes and the information systems and organizational infrastructure supporting those processes.
Expected Outputs	System Security Plan - specification of security controls that identify which, where, and how security controls will be applied.
Synchronization	Security controls and associated specifications should reflect appropriate levels of protection to the system in line with the security control selection criteria. Significant decisions should consider any possible secondary risks that may result should the decision influence previously considered security controls and protections identified during the risk assessment.

3. Design a Security Architecture:

Table 3-6: Design Security Architecture

Description	At the system level, security should be architected and then engineered into the design of the system. This may be accomplished by zoning or clustering services either together or distributed for either redundancy or additional layers of protection. Security designing at the system level should take into consideration services obtained externally, planned system interconnections, and the different orientations of system users. This activity can provide the most value for the system in lowering the total cost of ownership by planning the systems core components in a secure way.
Expected Outputs	Schematic of security integration providing details on where, within the system, security is implemented and shared. Security architectures should be graphically depicted and detailed to the extent the reader can see where the core security controls are applied and how. Listing of shared services and resulting shared risk. Identification of common controls used by the system.
Synchronization	The security architecture becomes a key component of the system documentation that should be reviewed and maintained as major changes or significant milestones are reached. Significant results from assessments, security testing, and reviews should be examined for potential feedback on effectiveness.

4. Develop a Security Documentation:

Table 3-7: Select and Document Security Controls

Description	The most prominent document is the System Security Plan. Development of these documents should consider the maturity of the security services being documented. In some cases, these documents may contain only known requirements, common controls, and templates. Filling in these documents should begin as early as possible during the project. Documenting as the system development progresses can provide cost savings and enhance decision-making capabilities through a comprehensive approach that allows early detection of gaps.

Expected Outputs	Additional security documentation supporting the system security plan.
Synchronization	These documents will need to be updated toward the end of user acceptance testing to ensure that they are accurate.

5. Conduct Testing;

Table 3-8: Conduct Testing

Description	Systems being developed or undergoing software, hardware, and/or communication modifications must be tested and evaluated prior to being implemented. The objective of the test and evaluation process is to validate that the developed system complies with the functional and security requirements.
Expected Outputs	Documentation of test results, including any unexpected variations discovered during testing.
Synchronization	All test results are returned to developers for configuration-managed updates. Unexpected results may require the customer to clarify the nature of the requirement.

Stage 3: Implementation:
Implementation/Assessment is the third phase of the SDLC. During this phase, the system will be installed and evaluated in the organization's operational environment.

Key security activities for this phase include:

- Integrate the information system into its environment;
- Plan and conduct system certification activities in synchronization with testing of security controls; and
- Complete system accreditation activities.

There are three key steps in this phase;

1. Create a Detailed Plan for Authorizing Officials;

Table 3-9: Create a Detailed Plan for Authorizing Officials

Description	The Authorizing Official (AO) is responsible for accepting the risk of operating the system; the AO can advise the development team if the risks associated with eventual operation of the system appear to be unacceptable. Specifications can impose excessive burden and costs if the acceptable residual risks are not known. The involvement of the AO is required for this determination of acceptable residual risks. It is easier to incorporate requirement changes during the planning stage of a system acquisition than during the solicitation, source selection, or contract administration stages. The possibility of establishing a security working group should be discussed. Such a group may consist of personnel such as users, program managers, and application sponsors; system, security, or database administrators; security officers or specialists, including the system or application analysts. To ensure proper testing and reduce the likelihood of scope creep during testing, the security accreditation boundary should be clearly delineated. This will form the basis for the test plan to be created and approved prior to implementation performance.
Expected Outputs	Initial Work Plan: A planning document that identifies key players, project constraints, core components, scope of testing, and level of expected rigor. The certification package should be close to completion, and any initial agency-specified conformance reviews initiated.
Synchronization	ISSO provides the system owner with completed documentation required to initiate and conduct such an authorization.

2. Integrate Security into the Established System;

Table 3-10: Integrate Security into the Established System

Description	System integration occurs at the operational site when the information system is to be deployed for operation. Integration and acceptance testing occur after information system delivery and installation. Security control settings are enabled in accordance with manufacturers' instructions, available security implementation guidance, and documented security specification.
Expected Outputs	Verified list of operational security controls. Completed System Documentation.
Synchronization	Issues encountered during installation should be evaluated for inclusion into the contingency plan based on the potential for reoccurrence.

3. Assess System Security;

Table 3-11: Assess System Security

Description	Systems being developed or undergoing software, hardware, and/or communication modifications must be formally assessed prior to being granted formal accreditation. The objective of the security assessment process is to validate that the system complies with the functional and security requirements and will operate within an acceptable level of residual security risk.
Expected Outputs	Security Accreditation Package, which includes the Security Assessment Report and the updated System Security Plan.
Synchronization	Certifier provides written Certification Package results to system owner, ISSO, and system administrator. Assessment results are shared with system owner, ISSO, system administrator, and developers.

Stage 4: Operations and Maintenance:

Operations and Maintenance is the fourth phase of the SDLC. In this phase, systems are in place and operating, enhancements and/or modifications to the system are developed and tested, and hardware and/or software is added or replaced. The system is monitored for continued performance in accordance with security requirements and needed system modifications are incorporated. The operational system is periodically assessed to determine how the system can

be made more effective, secure, and efficient. Operations continue as long as the system can be effectively adapted to respond to an organization's needs while maintaining an agreed-upon risk level. When necessary modifications or changes are identified, the system may reenter a previous phase of the SDLC.

Key security activities for this phase include:

- Conduct an operational readiness review;
- Manage the configuration of the system ;
- Institute processes and procedures for assured operations and continuous monitoring of the information system's security controls; and
- Perform reauthorization as required.

Here again, there are three basic steps to be dealt with, represented in table 3-12, table 3-13 and table 3-14;

1. Review Operational Readiness;

Table 3-12: Review Operational Readiness

Description	Many times when a system transitions to a production environment, unplanned modifications to the system occur. If changes are significant, a modified test of security controls, such as configurations, may be needed to ensure the integrity of the security controls.
Expected Outputs	Evaluation of security implications due to any system changes.
Synchronization	System Administrator and ISSO confirmation to System Owner that system is operating normally and compliant with security requirements. Should a last minute change occur that fundamentally changes the level of risk to the system, the system owner should consider recertification - this is rare.

2. Perform Configuration Management and Control;

Table 3-13: Perform Configuration Management and Control

Description	Configuration management and control procedures are critical to establishing an initial baseline of hardware, software, and firmware components for the information system and subsequently for controlling and maintaining an accurate inventory of any changes to the system. Changes to the hardware, software, or firmware of a system can have a significant security impact. Documenting information system changes and assessing the potential impact on the security of the system on an ongoing basis is an essential aspect of maintaining the security accreditation.
Expected Outputs	Change Control Board (CCB) decisions Updated security documentation Security evaluations of documented system changes.
Synchronization	System updates should be included into the system security documentation at least annually or with significant change. CM system documents should provide input into the Continuous Monitoring plan for the system.

3. Conduct Continuous Monitoring;

Table 3-14: Conduct Continuous Monitoring

Description	The ultimate objective of continuous monitoring is to determine if the security controls in the information system continue to be effective over time in light of the inevitable changes that occur in the system as well as the environment in which the system operates. A well-designed and well-managed continuous monitoring process can effectively transform an otherwise static security control assessment and risk determination process into a dynamic process that provides essential, near real-time security status information to appropriate organizational officials. This information can be used to take appropriate risk mitigation actions and make credible, risk-based authorization decisions regarding the continued operation of the information system and the explicit acceptance of risk that results from that decision. The ongoing monitoring of security control effectiveness can be accomplished in a variety of ways, including security reviews, self-assessments, configuration management, antivirus

	management, patch management, security testing and evaluation, or audits.
Expected Outputs	Documented results of continuous monitoring Security reviews, metrics, measures, and trend analysis Updated security documentation and security reaccreditation decision, as necessary.
Synchronization	Continuous monitoring should be adjusted as risk levels fluctuate significantly and security controls are modified, added, and discontinued.

Stage 5: Disposal:

Disposal, the final phase in the SDLC, provides for disposal of a system and closeout of any contracts in place. Information security issues associated with information and system disposal should be addressed explicitly. The disposal activities ensure the orderly termination of the system and preserve the vital information about the system so that some or all of the information may be reactivated in the future, if necessary. Particular emphasis is given to proper preservation of the data processed by the system so that the data is effectively migrated to another system or archived in accordance with applicable records management regulations and policies for potential future access.

Key security activities for this phase include:

- Build and Execute a Disposal;
- Archive of critical information;
- Disposal of hardware and software.

The three basic steps listed above are what mark the end to the properly planned and listed SDLC; table 3-15, table 3-16 and table 3-17 summarize this.

1. Build and Execute a Disposal;

Table 3-15: Build and Execute a Disposal

Description	Much like a work plan, this plan identifies necessary steps, decisions, and milestones needed to properly close down, transition, or migrate a system or its information. In many cases, disposed systems or system components have remained dormant but still connected to the infrastructure. As a result, these components are often overlooked, unaccounted for, or maintained at suboptimal security protection levels thus, providing additional and unnecessary risk to the infrastructure and all connected systems.

Expected Outputs	Documented disposal plan for closing or transitioning the system and its information.
Synchronization	Security documentation should reflect pending plans if security decisions and funding are reallocated or otherwise impacted because of the disposal decision.

2. Ensure Information Preservation;

Table 3-16: Ensure Information Preservation

Description	When preserving information, organizations should consider the methods that will be required for retrieving information in the future. The technology used to retrieve the records may not be readily available in the future (particularly if encrypted). Legal requirements for records retention must be considered when disposing of systems.
Expected Outputs	Index of preserved information, and its location and retention attributes.
Synchronization	Records management and Privacy Act requirements should be considered.

3. Dispose of Hardware and Software;

Table 3-17: Dispose of Hardware and Software

Description	Hardware and software can be sold, given away, or discarded as provided by applicable law or regulation. The disposal of software should comply with license or other agreements with the developer and with government regulations. There is rarely a need to destroy hardware except for some storage media that contains sensitive information and that cannot be sanitized without destruction. In situations when the storage media cannot be sanitized appropriately, removal and physical destruction of the media may be possible so that the remaining hardware may be sold or given away. Some systems may contain sensitive information after the storage media is removed.

Expected Outputs	Disposition records for hardware and software. These records may include lists of hardware and software released (sold, discarded, or donated), and lists of hardware and software redeployed to other projects or tasks within the organization.
Synchronization	Updating of system and component inventories.

3.1.4 Technical Best Practices for handling violations to Confidentiality, Integrity, Availability, and Accountability

Previous sections discussed general processes for secure systems. This section discusses technical best practices that can be used to enforce confidentiality, integrity, accountability, and availability policies. Information transferred in the Smart Grid systems could be manipulated by an attacker to affect grid reliability or cause large financial impacts to both utilities and energy consumers. For example, if an attack could successfully modify price information or meter information, customers' energy bills could be affected. Also, a customer could deny receiving some information which will result in a dispute between participants of the system or decrease in customer's confidence. Information must be protected from attacks such as eavesdropping, Man-in-the-Middle (MITM) attacks, and unauthorized access or modification of information. To do so, cryptographic schemes, such as Symmetric and Asymmetric algorithms, can be used to provide security goals – Confidentiality, Integrity, Availability and Accountability. Several authentication techniques can be used to verify the identities of the users in the system. Access control policies can also be used to provide authorization or specify privilege for users.

3.1.4.1 Use of Cryptographic tools

Confidentiality

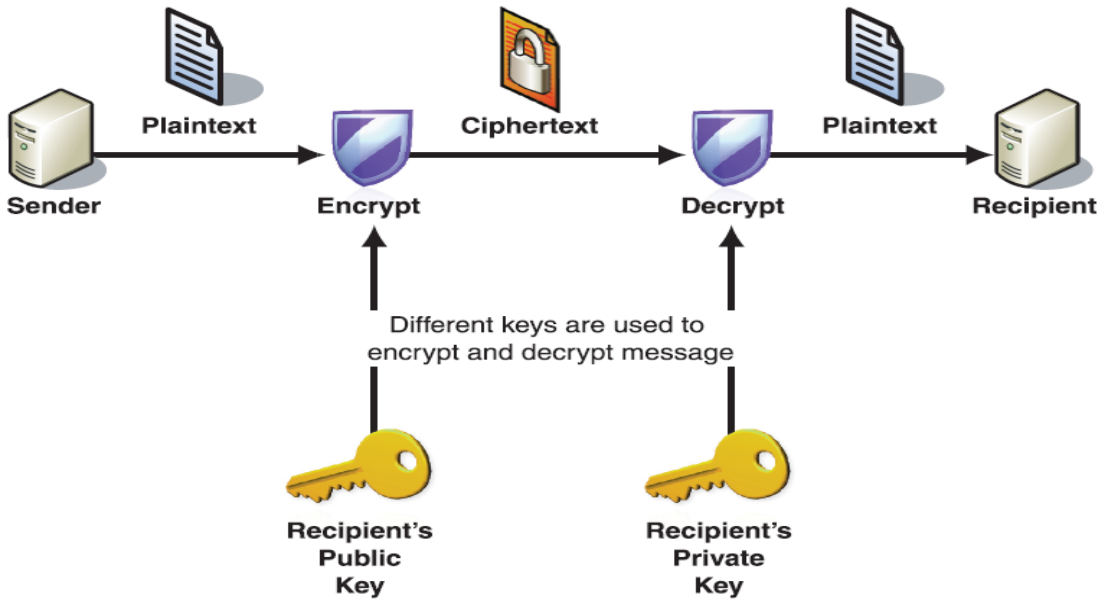
If an attacker can gain some customer information, such as energy usage or other personal information, the privacy of the customers will be invaded. Also, some critical information like Demand Response strategies should not be accessed or known by an adversary, since he/she can manipulate the information to extend some knowledge of the system and use that information to attack the system.

To provide confidentiality of the information, encryption techniques can be used. One of them is to use symmetric or shared key method. The information can be encrypted and decrypted by using shared secret key which is usually known by both sender and receiver. Thus, even if an attacker intercepts the information transmitted between the components in the system, the plaintext will not be discovered without the knowledge of the secret key. However, this approach has major flaws. One of them is that, in practice, the shared key may be distributed to more than two entities and hence it increases the chance for leaking of the key. Also, if the key is compromised, all the communication channels using that key will be no longer secure.

Moreover, the key distribution is extremely expensive and difficult to manage because every entity in the system must have shared keys to communicate with others.

Another approach is to use public key encryption to provide confidentiality of the information. This technique requires each entity has a pair of keys – Public and Private Keys. Public key usually is known by public, but private key is known by only its owner and will not be disclosed to anyone. Only the key pair can be successfully used to encrypt and decrypt the message. Even though these keys go in pairs, it is extremely difficult to derive one from the other. To encrypt the plaintext, the sender will use the public key of the recipient. Hence, the receiver will use his own private key to decrypt the ciphertext. The figure 3-2 below describes how to provide encryption and decryption using public key.

Figure 3-2: Public Key Encryption[66]



The public key encryption provides higher security level than secret key encryption because the private key will not be distributed to others and the only one who can decrypt the message is the owner of the private key. On the other hand, the computation of the asymmetric approach is more complex than that of the symmetric approach since the key size and ciphertext are much larger, so the performance of the system may be slower than using symmetric cryptography.

Additionally, in some system, the information can be real-time based, which means that the performance of the system must be of concern. Thus using asymmetric approach may not be

[66] Microsoft Developer Network (MSDN) library, Microsoft Corporation, "Web Service Security Scenarios, Patterns, and Implementation Guidance for Web Services Enhancements (WSE) 3.0", 2009 [online]. Available: http://msdn.microsoft.com/en-us/library/aa480545.aspx. [Accessed Dec 4, 2009]

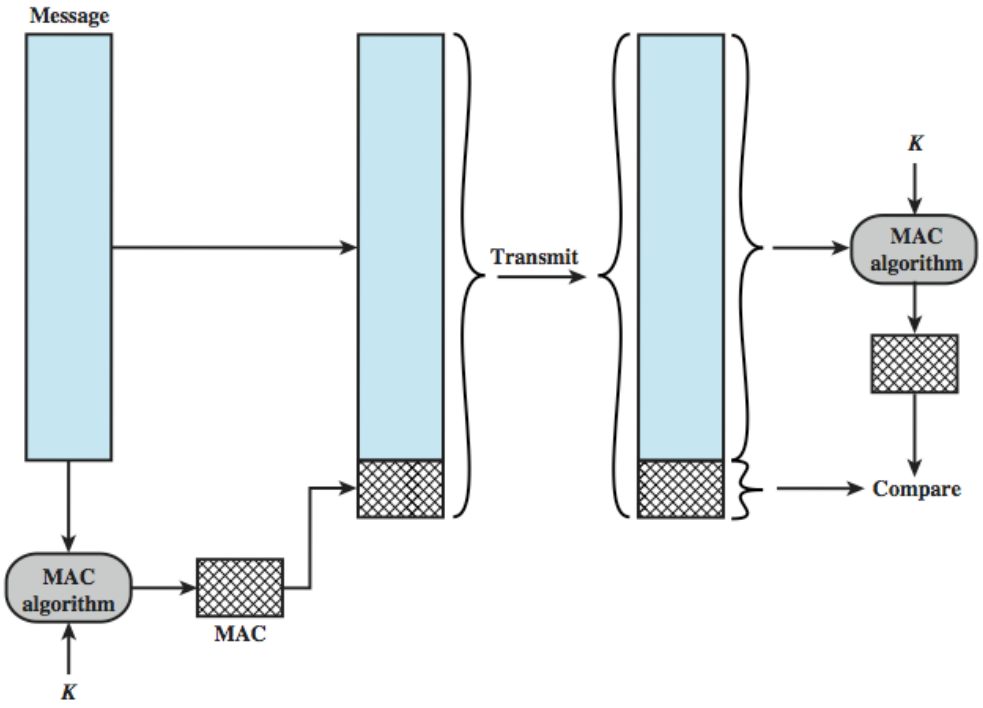
appropriate in that case. Another approach is to combine the use of symmetric and asymmetric cryptography. The public key can be used as a long-term key, while the shared key is used as temporary (or session) key. Before the communication takes place, both sender and receiver can exchange the session key by using the other end side's public key to encrypt the shared key. After the shared key is established, both sender and receiver use the shared key to encrypt and decrypt data for the communication. When the communication is ended, the shared key may be re-used or established again. This way the communication will not be delayed because of the size of the message and be secured since the session key will be used as a short-term key or one-time key.

Integrity

The term integrity can be used to refer to both source integrity (authentication) and data integrity (message integrity). If an identity of a source is not verified, an attacker can inject a false message into the system or the message can be come from a fraudulent source. Also, if the information sent in the system is modified, the system must be able to detect that a modification has been made. The impacts of the breach in this security goal vary from the grid itself to customers' billings. Man-in-the-Middle (MITM) attacks or other forms of unauthorized modification attack can be carried out, if the system fails to provide defensive mechanisms against those kinds of attacks.

In the symmetric approach, identities of both the sender and receiver are authenticated because only the sender and receiver know the shared key. Therefore, in some cases, the use of the shared key technique also provides source integrity. Message authentication can be provided using Message Authentication Code (MAC). MAC is authentication tag which is generated by applying MAC algorithm together with shared secret key and the message. MAC can be computed and verified by using the same key. Thus, the receiver uses the same shared key of the sender to verify if the message is modified or not. MAC algorithm can be done using Hash function. Figure 3-3 demonstrates the use of MAC for message authentication. The notation K in the figure referred to shared key between the sender and receiver.

Figure 3-3: Message Authentication Code[67]



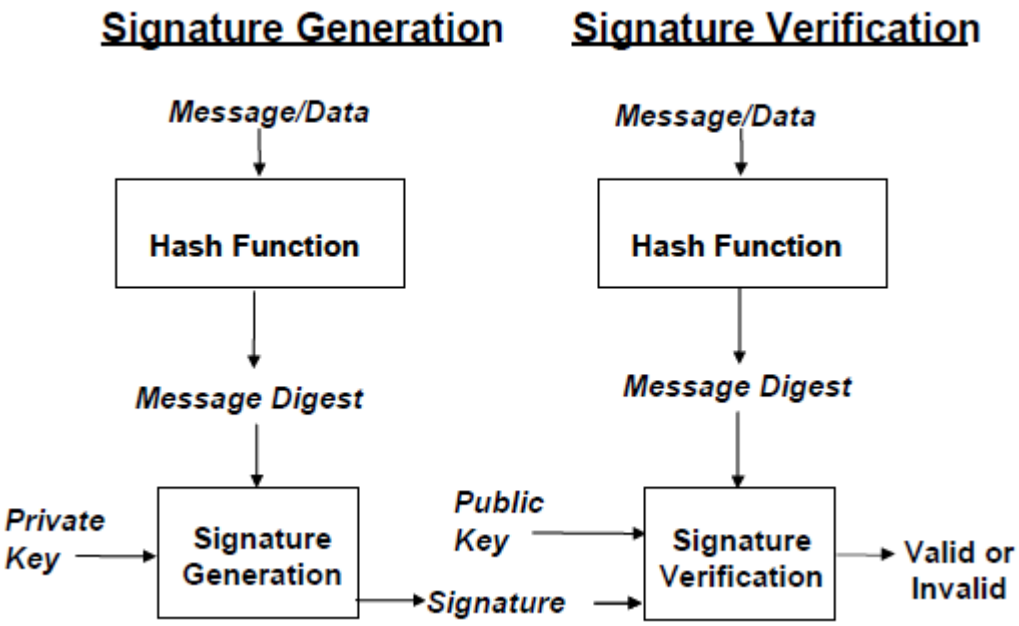
Thus, when the receiver can verify if the message has been modified by using the same MAC algorithm and shared key to compute MAC from the receiving message and compare it with the MAC part of the receiving message. If they are equivalent, the receiver can be sure that the message has not been modified.

Another way to provide integrity is to use asymmetric approach. In public key scheme, Digital Signature Algorithm (DSA) can be used to provide authentication and message integrity. Digital Signature is analogous to hand-written signature. However, it is very difficult to be counterfeited because it can combine the name and identity of the signer. The signature part is generated by using Secure Hash Function and the sender's private key. The sender encrypts the hash of the original message using his private key. When the message is received, the recipient verifies that the message has not been altered in transit using public key of the sender and the same hash function. The source of the message is authenticated, because only the corresponding public key can verify the signature. Thus, Digital Signature provides both source and data integrity. Figure 3-4 shows the process of signature generation and verification.

---

[67] W. Stalling, L. Brown , "Computer Security Principles and Practice: Chapter 2 – Cryptographic Tools", First Edition, 2008 [online]. Available: http://people.eecs.ku.edu/~saiedian/Teaching/Fa09/710/Lectures/ch02.pdf. [Accessed Jan 20, 2010]

Figure 3-4: Signature generation and verification[68]



One issue with the use of public key cryptography is that the public key must be certified. That is, one has to prove that it belongs to the intended user and is not a forged. For example, an adversary uses a public key with the name and identity of the intended recipient instead and uses this bogus key to communicate with the system. Digital Certificate can be used to ensure that the public key is authenticated and come from the source that it claims.

Typically, Digital Certificate contains a public key, the certificate information regarding the public key and the digital signature of a Certificate Authority (CA). The certificate information can be the name and identity of the public key or subject data, the algorithm used and date range which is considered valid of the certificate. The signature part of the certificate is derived from a public key and the credential of the public key owner and digitally signed with CA's private key. The recipient of the certificate uses CA's public key to verity the certificate. CA can be an internal or external organization or a trusted third party who can certify the public key associated with the name and identity of the owner. Thus, the use of certificate ensures that the public key in the certificate belongs to the owner or subject of the certificate. The use of digital certificates in the smart grid is a problem that will be discussed further in the next chapter.

[68] National Institute of Standard and Technology (NIST), "Digital Signature Standard (FIPS 186-3)", June 2009 [online]. Available: http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf. [Accessed Jan 20, 2010]

Availability

Availability of data is to have data available in a timely manner. In the Smart Grid system, some information, such as Real-Time Pricing (RTP) information and Demand Response events, is required to be accurate and available all the time. However, an attacker can perform Denial of Service attacks (DoS) which usually affect the availability of the system. Mutual authentication techniques could be used to reduce the number of DoS attacks since both client and server must authenticate each other before the communication takes place. However, an attacker still can flood the network with large amount of packets in order to exhaust the bandwidth limits, resulting in loss of availability. Therefore, cryptographic approaches alone are not enough to defend against DoS attacks. Other security measures, such as using Intrusion Detection System (IDS) and Firewall with Access Control list, applying secure software development methodology, using secure communication protocols, should be applied. Legacy devices at end user and low bandwidth of communication channels may result in the loss of availability as well.

Accountability (Non-repudiation)

When a user receives some information, such as price information, and performs some response based on the energy price received, there may be a risk that the user can deny receiving the information. Thus, the mechanisms for checking to see if the system already sent the information to the user and/or the user already received the information are necessary. The system must provide the means to ensure that the user is accountable for his or her action. The failure to provide accountability may result in a dispute between a user and the system provider and it also decrease the customer's confidence.

Digital signature technique can be used to provide accountability. Typically, a private key is only known by the owner and restricted from public. When a user receives the information which is digitally signed using DSA (digital signature algorithm), only the corresponding public key can ensure that the sender is the only one who signed the message. This could prevent the sender from successfully denying that he or she sent the information.

On the other hand, to prevent the receiver from denying receipt of the information, the response message which has to be signed by using the private key of the receiver is needed. The response message should include all the contents of the information received, plus the identity of the receiver, along with the signature part. The signature part is generated by using the private key of the receiver, the identity of the receiver and the secure hash function. Because the response message is digitally signed with the private key of the receiver, only the corresponding public key can ensure that the receiver is the only one who can sign the message. This can ensure that the receiver is held accountable for receiving the information.

To implement this technique in Smart Grid system, there must be some secure storage to keep the digital signatures of both sender and receiver. When a dispute takes place, the digital signatures stored in the storage can be used to verify accountability.

3.1.4.2 User Authentication

Before a user can gain access to any resources, such as files, processes, or data, of the system, the identity of the user must be successfully verified and the user must have the right to access those resources. The process of verification of the user's identity is called user authentication. After the user is authenticated, access control mechanisms can be used to check to see if the user is allowed to access the required resource. The detail of access control will be discussed later in this section.

Authentication can achieve in many ways, such as using password, biometric and public key cryptography, thus choosing the appropriate method is one of the crucial decisions in designing a system. This section is intended to provide commonly use authentication techniques.

3.1.4.3 Password Authentication

Passwords are the most widely used method for user authentication. In general, a user provides the identity and types some word, phrase or password he knows. The system compares the saved password with the received password for authenticating the user. Even though, this method is simple and easy to be implemented, there are vulnerabilities, which need to be addressed.

1. Password may be easy to guess, if the system does not provide security policies for creating user passwords, such as policies against using short passwords or common passwords that are easy to guess.
2. Password must be protected using encryption techniques and stored in secure storage.
3. Countermeasures for password attacks, such as password sniffing and password guessing attack, must be provided in order to reduce the risk of discovering password by an attacker.

Token Authentication

Token authentication attempts to use something that a user has, such as smart cards, magnetic stripe cards, memory card, cell phones, security tokens, etc., to authenticate with the system. This technique alone may not be secure enough for the system since the token can be stolen and used by an adversary. However, it can be combined with the password or PIN, which provides significantly greater security than using password alone. The use of token and PIN is called two-factor authentication.

Biometric Authentication

Biometric Authentication is the verification of an individual based on unique, physical characteristics, such as fingerprint, retina, iris patterns, voiceprint and signature. Biometric authentication provides higher level of security than password authentication, but it is technically complex and expensive compared to password authentication. However, the major advantage of using biometric is that it is not easily stolen or lost. However, to apply biometric method, types of biometrics have to be considered since they have advantages and disadvantages over the others. For example, voice patterns can be easily faked by using a

recorder, but it can provide a way to identity the subject without the subject's knowledge. Fingerprints may be unique and easy to implement, but the subject's finger needs to be clean, so it may not appropriate to apply to industrial applications.

Digital Signature

There may be some case where it is not necessary to authenticate the communicating parties. For example, when downloading music or software patch from the Internet, the server does not need to identify who is downloading, but may have to ensure the users that the data is genuine and is not tempered with by malicious software like virus or spyware.

3.1.4.4 Access Control/Authorization

Authorization refers to the act of granting a user or device proper right to access some particular resource of the system. Authorization fundamentally relies on authentication; thus, the process of authorization must take place after a user, device or subject is already authenticated. To provide authorization, access control mechanisms are necessary. For this reason, the two terms, authorization and access control, are sometime used interchangeably. Access control is used to limit authenticated user to gain an access to a particular resource, and prevent unauthorized use of a resource, such as viewing and modifying a resource, including use of resource in an unauthorized manner. Three most commonly used access control policies are Discretionary Access Control (DAC), Mandatory Access Control (MAC) and Role-based Access Control (RBAC).

Discretionary Access Control (DAC)

DAC is based on the identity of the subject, which can be a user, process or component, and on the access rules. The access rules to an object used to determine whether the subjects are allowed to perform are specified by the owner of the object or anyone who is authorized to control the access to the object. Access decisions are based on the credentials that the subject presented at the time it is correctly identified, such as username/password, biometrics, and cryptographic tokens. Typically, in DAC model, a subject may have an access right which allows enabling another subject to access to the same resource at the subject's discretion.

DAC is likely to be very flexible and simple, but there are two main issues that need to be considered in order to implement DAC policy. First, information of the object could be copied by the subject that is granted by the owner of that object. For example, Bob may grant Ann read access to some file, but if there is no mechanism to prevent Ann from copying the content of the file, she may be able to copy and use that information in an unauthorized manner. Second, the access rights to an object are controlled by the owner of the object, rather than controlled by the system authority who manages the system security policies.

Two most commonly used mechanisms for implementing DAC policy, which could be used in Smart Grid, are Access Control List (ACL) and Capability List (CL).

1. ***Access Control List (ACL)*** is a list of permissions associated with an object that is used to specify which subjects, users or systems are allowed to access that particular object as

well as which operations the subject can perform on that particular object. Each entry in ACL is called Access Control Entry (ACE) which is usually composed of an identity of the subject and set of the permissions being granted or denied for that object. In the ACL-based environment, it is simple to determine which users that are allowed to access to this particular object. However, it is difficult to determine all the access rights for a particular user. Thus, in some environment with the large number of users, where the change in access control policies could be occurred constantly, implementing ACL may not be appropriate. ACL could be created and stored in devices. If an access to a particular device is attempted by some users or devices which are not in the list, the access must be denied. By checking access rights for each object the user has, ACL can be used to protect against an unintended operation performed by legitimate users or devices as well.

2. ***Capability List (CL)*** A capability can be viewed as a token, a key or a ticket of an object associated with the permission to access that object. A capability can be analogous to a movie ticket which a customer must have to access into the movie theater or a key that is needed to enter the house. In capability-based system, a subject, which is requesting an access to a particular object, must possess a capability for that object in order to gain access to the object. A capability could be delegated to anyone else by the owner of the object, which is analogous to the movie ticket or the key which could be given to another. Thus, capabilities are critical to the system security, so when the capability is given to the subject, it must not be tempered by that subject.

Mandatory Access Control (MAC)

MAC is an access policy used in multiple-level systems that require highly sensitive data, such as classified military or government information. MAC ensures the enforcement of security policies by assigning labels on the information and comparing it to the level of sensitivity a subject has. A subject can only access to the data on which it has a label. For example, a user whose label is the "Secret" classification should not be able to read a file of which the label is the "Top Secret" classification. The owner of the object cannot change the access rights to that object; thus, the access decisions are made by a central authority of the system, not by an individual owner.

Role-based Access Control (RBAC)

RBAC is based on the roles or responsibilities that a subject or a user has within the organization and on rules which determine what access rights are permitted for the subject in a given role. Access rights are grouped by role name and the operations on which an individual user can perform are based on the associated role. Typically, the process of defining roles is based on security policies derived from analyzing fundamental goals and structures of the organization.

In RBAC, users are granted membership by determining their responsibilities into roles. When a new user account is created to the system, it has to be assigned into a proper role. Therefore, assigning user membership into roles can be easily established as a job assignment. An old

operation associated with a particular role can be deleted and a new operation can be established easily without affecting other roles. A user with a given role will not be able to perform any operation other than the operations which are not assigned into that role. Therefore, the use of role to control accesses can be very effective since roles can be modified without updating the access rights for each of the users in the system. However, sometime, several operations in one role could be overlapped with others, so the principal of the least privilege, which will be discussed later in section 3.1.5, must be applied such that the user should be given no more than the privileges that are necessary to complete his or her tasks.

Access Control and Smart Grid Communication

The access control policies are tailored to the requirements of networking and communication. In the smart grid systems, different types of networks, such as Enterprise Bus, Wide Area Network (WAN), Field Area Network, etc. could be implemented. These networks may be implemented using public networks, such as Internet, and non-public network. The communication may go through both public and non-public networks. The communication from public networks should be able to access least resources or services than that of private networks. For instance, Field Area Network that could be used to connect the energy services interface and the meter in the customer domain, must have the access control which specifies what accesses are allowed and which operations can be performed. If the access control is not specified properly, an attacker may gain access to the meter remotely, and cause malicious impacts on the customer domain.

Also, each entity in the smart grid systems, such as Advance Meter Infrastructure (AMI), Home Area Network (HAN) or Neighborhood Area Network, is required to have appropriate access control policies in order to restrict the incoming and outgoing connection to the devices within the network. The policy must be specified in such a way that which communication from/to which entity should be allowed. For example, the connection from public network should be limited to access the resource in the AMI system while the connection from HAN to NAN could be allowed in a secure manner. ACL could be used in this environment in order to accept or deny the access from/to different networks.

Moreover, since there will be different kinds of personnel and device who can access and utilize resources in smart grid systems and perform different operations on those resources, the access control policies should be specified in the level of applications or devices. For example, utility operator may be able to perform configuration of the meter remotely, while the customer should be able to only view the price information from the meter. RBAC could be used in this situation by specifying the roles by determining the responsibilities as parts of the system. Thus, different entries, such as a home user or utility operator, who are assigned to different roles, will not be able to perform operations other than its own role.

The main purposes of access control are to ensure that the resource is only allowed for an intended user or device and that the user or device is identified. Limiting the permissions of the subjects such that the subject should be given only necessary privileges to complete its tasks

will help reduce the impact of unauthorized access and modification to the resource of the system. This principal is also called Least Privilege, which will be discussed in the section 3.1.5.

3.1.5 Secure System Design Principles

This section discusses general principles used in designing secure hardware/software systems. These principles can be used in any phase of the secure system life cycle. In general, these design principles of secure system are mostly based on simplicity and restriction. Simplicity refers to ease of use and ease of understanding the system. It relies on the fact that the simpler the system is, the less can go wrong. Restriction is used minimize permission granting to any entity in the system to access to the resources. There are eight principles discussed as follows:

1. ***Least Privilege:*** An entity or a subject must be given only the privileges that are necessary for its tasks, but no more. This principle ensures that even if, an attacker successfully gains access to some part of the system, it is still difficult for it to gain access to the rest of the system. Thus, this principle can reduce the impact of a failure when some part of the system is compromised. Also, the security analysis of each entity will be simplified since it only has minimal privileges. This principle can be used in all parts of the smart grid infrastructure.
2. ***Fail Safe Defaults:*** A failure of the system should not lead to any change in the system which leads to an insecurity state. This principle ensures that even if the system fails, it is still safe. This principle is used to design firewalls. That is, it will deny all the access by default. Access is granted only to subjects that are permitted.
3. ***Economy of Mechanism:*** A design should be as simple and small as possible. When the design or security mechanisms are highly complex, it is likely that the vulnerabilities of the system will be increased. Also, when an error occurs, it will be more difficult to detect. Simplicity refers to all aspects, such as design, implementation, specification, operations, etc. Each tool or component should be designed such that it performs a task in as simple a way as possible.
4. ***Complete Mediation:*** All accesses to every entity in the system must be checked to ensure that subjects have a permission to access that entity. This principle ensures that every access to the system will be authorized beforehand. If the permissions of the objects are changed, the update should be systematically done. A perimeter firewall is an example of a network system that can be used to check all accesses to an internet
5. ***Open Design:*** Security cannot rely on obscurity of its design or implementation. The security may be enhanced by the secrecy of design and implementation, but if the design is exposed, the security must not be affected. However, this does not mean that source codes of the programs, cryptographic keys, or any secret information of the programs should be published. Nevertheless, publication of source code can help enhance security because the system can be tested by a wider audience allowing vulnerabilities to be fixed.
6. ***Separation of Privilege:*** The system should not grant the privileges based on a single condition. This principle is used to ensure that multiple conditions are met before granting the access to resources. For example, an additional internal firewall is needed

for a critical component even if an external perimeter firewall is used for an entire system. Thus, even if an attacker gains one condition, he should not be able to gain permission to any entity. This principle is also known as defense in depth. It is used in several other situations such as multi factor authentication. The latter allows authentication to be implemented using multiple techniques such as physical presence: retina scan, fingerprint, smart card, etc. and other technically sound methods such as passwords protection.

7. ***Least Common Mechanism:*** Multiple subjects should not share mechanisms for access to any entity or resource of the system is an unauthorized manner. This principle minimizes the dangers of sharing state among different processes and programs. Thus, every shared mechanism must be designed in such a way that there is no unintentionally compromising security by another. This principle is the reason why isolation is used to ensure security. For instance a 'honeynet' can be used to attract attackers so that their modus operandi can be determined. It is important to use this principle to ensure that an attacker does not use the honeynet to attack a production network.
8. ***Psychological Acceptability***: A security mechanism should not introduce complexity of accessing the system. This principle is based on a human interacting with the system. The more complex interfaces the system has, the more mistakes the user can make. The designer should ensure that the human interfaces are designed for ease of use so that the users can apply or define security rules without misunderstanding. Also, the installation and configuration of the program should not be complex and when error occurs, the error messages should be easy to understand. This is the principle that should be used for password management. For instance if users are forced to choose very difficult passwords, change it too often, etc. they might find it unacceptable and either write recycle or choose/simpler ones. This principle means that employee concerns should be heeded when implementing security.

3.1.6 Conclusion

This chapter discussed general information security best practices that can be used in securing information systems. Applications of these principles to smart grid are mentioned where necessary. The best practices discussed involved all facets of a typical system: people, processes, and technology. The rest of this chapter discusses best practices for securing important components of the smart grid system using some of the principles discussed in this chapter. The best practices for securing the important smart grid components, namely Demand Response, Customer Domain Systems (i.e. Home Area Networks, Gateways, and Neighborhood Area Networks), Advanced Metering Infrastructure, Grid (Supervisory Control and Data Acquisition and Distributed Network Protocol), Plug in Electric Vehicles, and Distributed Energy Resources (DER) are discussed in the chapters through section 3.2 to 3.7.

3.2 Demand Response Best practices

3.2.1 Introduction

Demand Response (DR) systems are expected to be eventually utilized in most residential and commercial energy consumers. The security and privacy of customer information must be the highest priority. Proper data handling practices must be carried out in order to protect the security and privacy of customer information. The breach in security goals – confidentiality, integrity, availability, accountability – could adversely affect large scale of a smart grid system and large number of customers. The impacts are varied from the reliability of the grid itself to the financial impacts on utilities and customers as well as the invasion of the privacy of customer information. Consequently, it is important that security concerns and countermeasures are considered at the early stage. This section describes the security concerns in DR and DR network architecture like Sensor Networks. Also, it proposes security measures to defend against possible attacks based on the security concerns specified in this chapter. Finally, it provides best practices for security purposes related to the DR and Open Automated Demand Response (OpenADR) contexts.

3.2.2 Demand Response Security Concerns

This section is an overview of the security concerns on the major pieces of the information transmitted in DR systems included pricing signal, DR events information and bidding information.

3.2.3 Pricing Signal

The pricing signal consists of real-time pricing (RTP) and time-of-use pricing (ToU). Real-time pricing requires computer-based response, while the fixed time-of-use pricing may be either manually handled by the customer or automatically handled by the smart device based upon the time periods and the prices.

- Real-time price is the electricity prices that fluctuate during different time periods over the course of the day. This dynamic pricing allows customers (industrial, commercial and residential) to shift or shed electricity usage in order to minimize electricity and operating costs for their business. This price signal will show the current price for power and an automation system, such as smart clients or meters, will determine what actions need to be taken based on the pricing signal it received.
- Time-of-use price is the electricity prices that are not real-time. This pricing information is defined ahead of time, usually for 24 hour day, and fixed in the certain time periods based on seasons. For example, weekday afternoon in the summer the price is usually on-peak and weekend night during the winter the price is usually off-peak.

Since the real-time pricing information could be daily transmitted via the Internet, it has more security concerns than that of the fixed pricing. The integrity of the price information is of the most concern. The real-time price could be modified by an attacker in such a way that it affects the organization or customers financially. The modification of the price signals could affect the reliability of the grid. For example, if an attacker modifies the actual price information to be lower than the normal price, the building automation system may shift the electric loads and

the blackouts may occur. The automation system at customers' point must be able to authenticate that the price signals it received is actually come from the utility and not modified by an unauthorized entity. Moreover, confidentiality should be an issue. Eavesdropping on this information, especially the response information that customers make according to the power price, could reveal the electrical usage and invade the privacy of the customer. The customer also may deny receiving price signal or refuse to hold for his action in the response to the price signal. Thus, non-repudiation mechanism needs to be provided. Also, when it comes to real-time based services, the availability of the price information in timely manner could be issue as well.

The fixed time-of-use pricing is less concerned about the confidentiality and integrity of information, since the information is fixed for a certain period of time and is not regularly sent electronically. Thus, the meter reading and the accuracy of data should be only two concerns for ToU pricing.

3.2.3.1 DR Events Information

DR strategies are pre-programmed in Energy Management Control System (EMCS) at the customers' sites. The strategies are carried out when the DR events and pricing signal arrives. The main purpose of the DR strategies is to control the electric loads at the end users according to the electric demands in return for decreasing electric usage at end points and providing reliability to the grid. However, if DR events information is manipulated by an attacker by controlling the electricity usage, such as turning on/off the air condition or heating units at end users, this could affect both the utility and participants in DR program financially. Moreover, if an attacker turns on all air conditioning or heating units in a large commercial area, the excessive loads in the grid could occur, leading to blackouts and large financial impacts. In some case, the manipulation of DR events may affect health and safety of customers. For example, an attacker may turn on heating units during an extremely hot day in the summer. This type of attacks can be carried out by Man-in-the-middle (MITM) attacks.

An attacker may attempt to prevent EMCS at customers' sites from receiving the DR event signals from the utility gateway so that the EMCS cannot shed or shift electric loads. This type of attacks can be carried out by Denial of Service attacks.

The DR events information must be protected from any kind of unauthorized modification and the clients or EMCS must be able to authenticate that the DR signals are come from the legitimate source.

3.2.3.2 Bidding Information

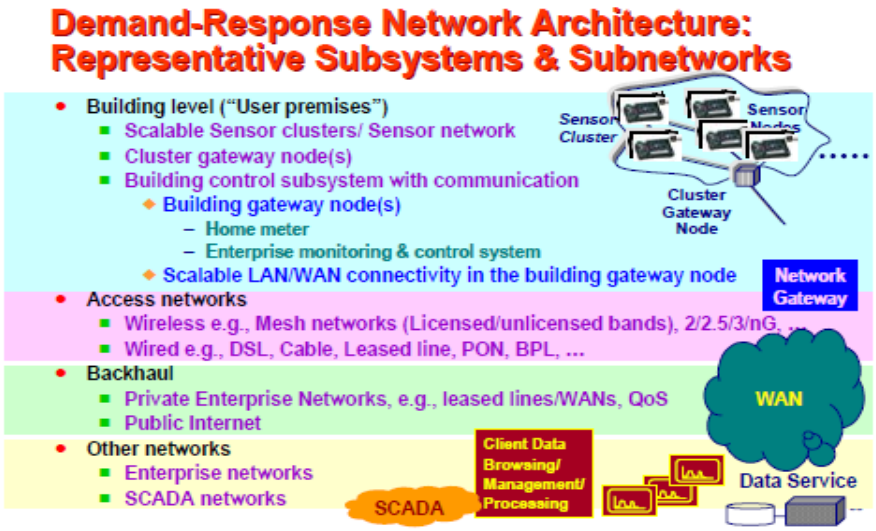
DR supports several bidding-based programs, such as Capacity Bidding Program (CBP) and Demand Bidding Program (DBP), which are offered through a utility, such as PG&E. Customers, who participate in these bidding programs, can submit a bid for load reduction for a purposed level of curtailment or against the energy generation resource. In return, the customer will get incentive payment, if the bid is cleared and he reduces the energy consumption according to the bid. The details of how each bidding program works are not in the scope of this paper.

The bidding process begins with the request for a bid from electricity generator, which could be sent in the form of an email, SMS, or by webpage. The customer submits request a bid to the generator. If the bid is accepted, the notification message will be sent to the customer via email, SMS or webpage. However, an attacker can also make a request for a bid or send notification messages by spoofing emails or SMS messages to the customer himself. Also, an attacker could manipulate the load reduction per time block information sent by the customer, causing false behavior of bidding program and financial impacts on bidding participants. For example, an attack pretends to be a customer and issues bidding message instead. Eavesdropping on the load reduction per time block information sent by customers could disclose the energy usage of the customer as well.

3.2.4 Demand Response Network Architecture

This section is to review some of the network architecture used in DR systems and analyze security concerns in the DR sensor network. Also, it provides security measures to the security concerns specified in this section.

Figure 3-5: Subsystems & Networks in a Sensor Network Based DR Architecture[69]



3.2.4.1 Subsystems and networks in Demand Response Sensor Networks

Demand Response sensor network consists of the followings:

- Sensor clusters or sensor network is a collection of sensors and actuators at either a residence, commercial or industrial building that has the ability to monitor and respond

[69] D. K. Mulligan, D. Wagner, U. Shankar, P.A. Subrahmanyam, E. Jones, J. Lerner. "Network Security Architecture for Demand Response/Sensor Networks". Technical report, On behalf of California Energy Commission, Public Interest Energy Research Group, January, 2005 [online]. Available: http://www.law.berkeley.edu/files/demand_response_CEC.pdf. [Accessed Nov 30, 2009]

to physical or natural conditions. The communication of each sensor node is based on wireless communications and can be used to receive DR and price signals and send relevant information, such as energy usage or sensor status. However, it has a limited set of computational tasks, including local data aggregation and encoding.

- Cluster gateway node acts as the proxy for each sensor cluster.
- The home or building control subsystem consists of one or more building gateway nodes, sensors and enterprise monitoring & control subsystems. The building gateway node can have scalable LAN/WAN connectivity includes:
    - Wired network such as DSL, Cable, Leased line or Passive Optical Networks (PONs)
    - Wireless network such as cellular network (2, 2.5, 3, 4G) operating in licensed frequency bands IEEE 802.11x networks as well as Mesh networks.
- Backhaul Networks can be private enterprise networks, such as leased lines, WAN, or public Internet.
- Other networks, such as SCADA networks.

3.2.4.2 Sensor Networks and Security Concerns

Sensors have the capabilities of observing information, such as temperature, lighting and humidity and forwarding a response based on the information received to EMCS. For example, in the area that has comfort temperature, air conditioning units may be turned down. Pricing signals can be specified based on sensor data a utility receives as well. However, an attacker may inject some sensor data or disrupt sensor reading which can cause false sensor reading and an inappropriate response to EMCS. Also, some malicious command, such as turning on heating units during the summer, could be inserted into the sensor nodes. This can affect billings and/or health concerns of the customers. The limitation of sensor nodes, such as slow CPUs, short battery life and small memories, should be a concern as well. In order to provide security goals, advanced cryptographic tools must be used; however, complex computations may shorten the battery life and may be slow due to the limited CPUs and memories. The limitation in battery life of the sensor nodes exposes another attack that tries to drain power of sensor nodes by sending a number of messages to them since they have to authenticate and verify each message. Thus, the sensor nodes must not perform much computation on the collected data in order to prolong the battery life. Also, physical attack to a sensor node could make an attacker obtain the keys embedded inside.

3.2.4.3 Sensor Networks and Security Measures

This section provides security measures in order to defense against the attacks specified in 3.2.2.

Use of Cryptography

If an adversary can capture one or more packets and analyze traffic, he may inject false messages or modify the contents. The system must have the ability to prove that a message comes from the source that it claims and the message has not modified in an unauthorized manner. Many cryptographic approaches could be used to provide particular security goals.

One of them is to use symmetric key (shared key) approaches and separate shared keys for each pair of nodes. The node can only communicate with its pair because it requires the same key to encrypt and decrypt the message. Thus, both receiver and sender node can authenticate each other because they have the same shared key. If one of the nodes is compromised, an attacker cannot impersonate the other pair nodes since each pair of nodes requires one shared secret key. To implement this approach, the key has to be distributed ahead of time. Kerberos can be used for the key management and distribution. Data confidentiality is achieved by encrypting the message with the shared key. However, this approach may not be able to support non-repudiation. It also has high communication and implementation costs. Moreover, the battery life for this approach should be of concern since it can be shorter than it is expected to be. This leads to more attractive approach which can be used for sensor-class nodes.

Overview of Elliptic-Curve Cryptography (ECC)

Since sensor networks have the resource limitations, ECC can be an attractive approach which offers the same capabilities of cryptographic schemes used in the Internet communications, such as Digital Signature Algorithm (DSA) and Diffie-Hellman (DH) algorithm, but with the smaller key size. According to RSA Laboratories[70], Rivest, Shamir & Adleman Public Key cryptography (RSA) with 1024-bit key provide equivalent security level to ECC with 160-bit key. However, RSA laboratories recommend using RSA with 2048-bit key which is equivalent to ECC with 224-bit key to protect data beyond the year 2010[71]. ECC also offers Elliptic-Curve Digital Signature algorithm (ECCDSA) and Elliptic-Curve Diffie-Hellman (ECCDH) key exchange which makes it possible to provide mutual authentication, key exchange and ECC-based digital signature for Wireless Sensor Networks (WSN).

Use of ECC in Sensor Network

Authentication

Each sensor node must be able to detect that a message comes from an alleged source and the message has not been modified in an unauthorized manner. Mutual authentication approach can be used to provide such detection. Each sensor node can have its own public and private key pair. According to A. S. Wander[72], an abbreviated X.509 certificate can be imitated by having a unique node identity along with a public key and a signature. Hence, the ECC-based Secure Socket Layer protocol (SSL) can be implemented. Also, since ECC is based on Public Key

---

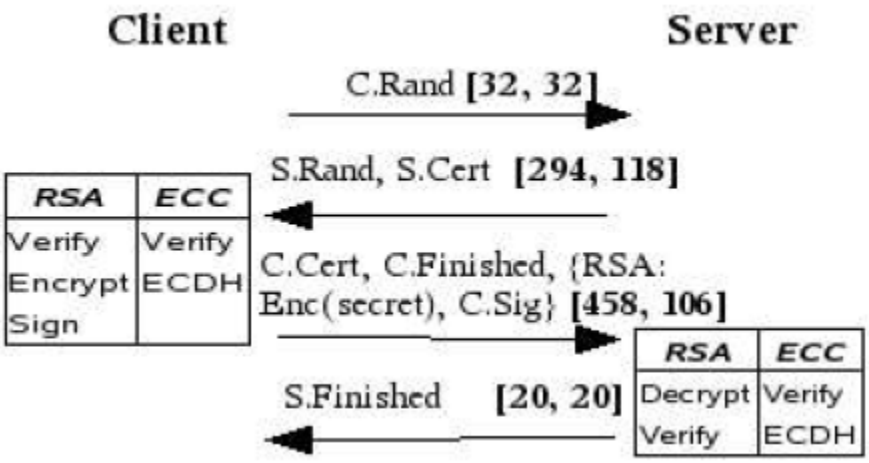
[70] M.J.B. Robshaw, Y. L. Yin, "Overview of Elliptic Curve Cryptosystems", RSA Laboratories Technical Note, June 1997. Available: http://www.rsa.com/rsalabs/node.asp?id=2013. [Accessed Dec 05, 2009]

[71] B. Kaliski, "TWIRL and RSA Key Size", RSA Laboratories Technical Note, May 2003 [online]. Available: http://www.rsa.com/rsalabs/node.asp?id=2004. [Accessed Dec 05, 2009]

[72] A. S. Wander; University of California at Santa Cruz, N. Gura, H. Eberle, V. Gupta, S. Chang, C. Shantz; Sun Microsystems Laboratories "Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks", March 2005 [online]. Available: http://research.sun.com/projects/crypto/wandera_energyanalysis.pdf. [Accessed Dec 05, 2009]

Cryptography, the only phase that affects when applying ECC to SSL is the handshake phase. Figure 3-6 demonstrates the exchange of message between the client and the server during the SSL handshake with mutual authentication for both RSA-based and the ECC-based SSL. The brackets [RSA, ECC] in the figure denote the size of the message in bytes for each algorithm. The notation C means the client and S means the server.

Figure 3-6: Simplified RSA-based and ECC-based



SSL handshake with mutual authentication; Pay load message size in byte [RSA, ECC]

The programmatic details of the message exchange during the ECC-based SSL handshake protocol is not in the scope of this chapter. The steps of the simplified version of ECC-based SSL handshake involve:

1. The client sends a 32-byte randomly generated number or data to the server.
2. The server replies back with the random data received from the first step along with the server's certificate. The server's certificate contains server's ECDH public key signed by Certificate Authority (CA) using ECDSA signature. If client successfully authenticate the server, the client uses its own ECDH private key and the server public key to perform an ECDH operation to gain the premaster secret. (Note that for RSA-based algorithm, the message size is 294 bytes while it is only 118 bytes for ECC-based algorithm)
3. The client sends its own certificate to the server. Also, the server performs an ECDH operation using its own private key and the client public key.
4. The derivation of the master key and session key is unchanged from the RSA-based SSL handshake.

To implement this approach, a base station, which acts as a control center or Certificate Authority (CA), is needed for collecting each node's public key certificate. This mutual authentication approach can authenticate whenever a new node is set up in a sensor cluster or network. In other word, the public keys of all the nodes are needed to be authenticated. Thus, if an attacker tries to set up his own sensor node to intercept the data sent in the sensor networks,

he will need to have a certificate, which is usually protected from an unauthorized access to the data in the certificate storage. However, this approach requires each node to keep its pair node's certificates on its memory; therefore, the size of the certificate should be of concern. (Note that, according to V. Gupta[73], a traditional X.509 RSA-1024 certificate is on the order of 700 bytes long, the simplified certificate is only 262 bytes long and an ECC-160 certificate can be reduced from approximately 530 bytes to 86 bytes) Also, the message authentication can be achieved by using digital signature. The use of digital signature can substantially reduce the impacts from Man-in-the-middle (MITM) attacks. The further detail of ECC Cipher Suits for TLS is specified in RFC 4492[74]

Confidentiality

Once the mutual authentication and key exchange between each pair of nodes are established, the shared key can be used to communicate with its pair node. If one of the pair nodes is compromised, the information sent between the other pairs of the node is not revealed since each pair of nodes have different shared key obtained during the key exchange phase. Also, the shared key should be re-established periodically in order to reduce the risk of an attacker gaining knowledge of the key. However, this means the sensor node needs to keep its pair node's shared key in its memory. This also can be an issue, since the memory size is limited. (Note that, according to RFC 4492[75], ECC with 160-bit key requires 282 bytes of data memory)

Accountability (Non-Repudiation)

Non-repudiation can be provided by using the digital signature technique. The details of how to provide accountability is discussed in the section 3.1.4.1.

3.2.4.4 Demand Response and Home Area Network (HAN)

Demand Response systems highly depend on Advanced Metering Systems which provide real time communication link between electric, gas, and water meters. This has led to architecting Home Area Networks that connect thermostats, load switches and lightening devices. All these smart devices connected to HAN can be set to operate during low cost energy period.

---

[73] A. S. Wander; University of California at Santa Cruz, N. Gura, H. Eberle, V. Gupta, S. Chang, C. Shantz; Sun Microsystems Laboratories "Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks", March 2005 [online]. Available: http://research.sun.com/projects/crypto/wandera_energyanalysis.pdf. [Accessed Dec 05, 2009]

[74] Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS) are available at: http://tools.ietf.org/html/rfc4492

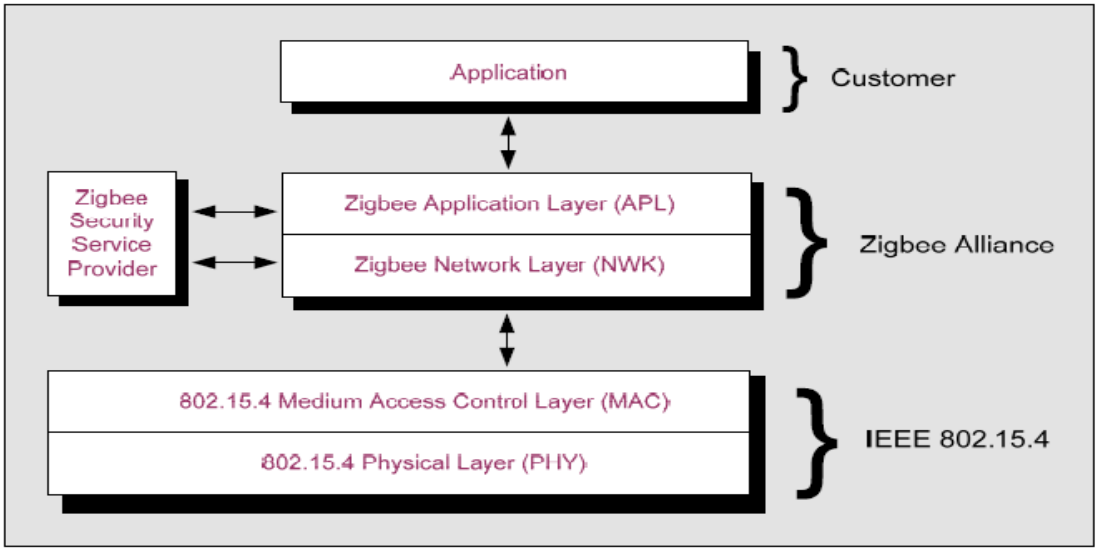
[75] A. S. Wander; University of California at Santa Cruz, N. Gura, H. Eberle, V. Gupta, Sheueling C. Shantz; Sun Microsystems Laboratories "Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks", March 2005 [online]. Available: http://research.sun.com/projects/crypto/wandera_energyanalysis.pdf. [Accessed Dec 05, 2009]

Introduction of HAN along with advanced wireless home networking has enabled use of home monitoring devices and home automation. The Zigbee wireless communication can be used in home automation for controlling demand response events. This section provides an overview of Zigbee standard and security issues of using Zigbee in HAN in Demand Response context. Also, it provides security measures against the issues specified in this section. This chapter does not intend to provide comprehensive details of the Zigbee protocol, but rather to provide enough information to discuss about the security issues and measures in the Demand Response context.

Overview of Zigbee Networking Standard

Zigbee is a low-power wireless networking standard which is built on top of IEEE 802.15.4 standard. It is designed specifically for wireless control and monitoring network and can be used to implement HAN devices and appliances in order to provide automation system in the home. Zigbee enables devices to self-assemble into wireless mesh network – from smart meters to devices in home. Zigbee provide two extra security layers which are built on top of IEEE 802.15.4 standard, where the security features are provided. The layers are network and application security layers. The figure 3-7 shows the Zigbee security layers.

Figure 3-7: Zigbee Layer Model[76]



[76] K. Masica; Lawrence Livermore National Laboratory, Recommended Practices Guide For Securing ZigBee Wireless Networks in Process Control System Environments (Draft), April 2007 [online]. Available: http://csrp.inl.gov/Documents/Securing%20ZigBee%20Wireless%20Networks%20in%20Process%20Control%20System%20Environments.pdf. [Accessed Jan 02, 2009]

Zigbee is based on 128-bit Advance Encryption Standard (AES) algorithm and the Counter Mode with Cipher Block Chaining Message Authentication Code protocol (CCMP). The 128-bit key, which is recommended by NIST[77], is considered relatively strong for AES algorithm. Zigbee supports security services, such as access control and frame integrity in order to provide authorization and data integrity. Also, it defends against replay attacks by comparing the sequential freshness value with the last known value and rejecting the data frame that has been replayed (or has the freshness value that has not been updated).

The cryptographic keys in Zigbee can be categorized into three groups as follows:

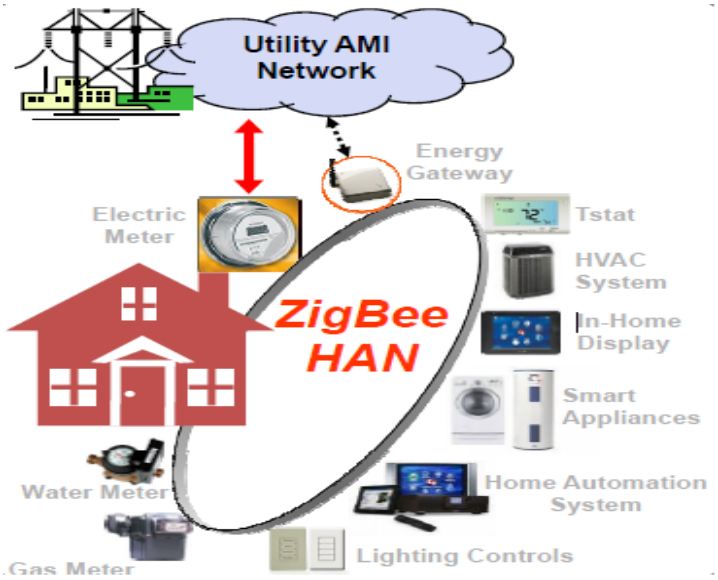
- Master Key is a long-term key used to establish symmetric keys (Link keys) between two Zigbee-enabled devices. The master keys are pre-installed in the devices by manufacturers in each device or are sent over-the-air to the devices.
- Link Key is unique session key between each pair of devices. The link keys are used to encrypt and decrypt information transmitted between each two devices in the HAN. Link keys are managed by the application layer.
- Network Key is a 128-bit key shared among all the nodes in the network. The network keys can be regenerated by the trust center or coordinator at different period of intervals. The network key is used by each node in order to join the network. It is used for broadcast communication in the network. When the trust center changes the network key, the old network is used to encrypt the new one and it is distributed throughout the network. Each pair of node can have both link key and network key. In this case, the network key will not be used since the link key is more secure.

Use of Zigbee-based HAN in Demand Response

The use of Zigbee in HAN enables electric consumer and utilities manage energy consumption effectively. For example, during the period of peak electrical demand, AMI system and HAN would work together and shed the load based on the price signal or DR events received by the utility in order to manage the high-load devices, such as changing the thermostat setting of the HVAC system in participating homes. The figure 3-8 demonstrates the high-level view of Zigbee-based HAN.

[77] Federal Information Processing Standards Publication 197"Advance Encryption Standard (AES)", Nov 2001 [online]. Available: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf. [Accessed Jan 03, 2009]

Figure 3-8: ZigBee-based HAN enabling demand response from utilities network[78]



The electric meter serves as the gateway, called Energy Service Portal (ESP), between Zigbee-based HAN and (Neighborhood Area Network) NAN or the utility. The ESP communicates with a variety of Zigbee-based devices, including Programmable Communicating Thermostat (PCT), In-home display, Energy Management Consoles, etc. The devices in HAN can receive pricing signals from the AMI network. Load control events which are typically created by the utility can be displayed in the in-home display and allow the utility to schedule turning off high-load applications, such as air conditioners and pool pumps, of the homeowners to manage energy and provide the reliability of the grid. Homeowners still can choose to opt-in or opt-out the events received based on the energy price during the peak demand.

After the utility sends DR events to the ESP, the events will be forwarded to the devices which are responsible for the signals. For example, load control device, which is responsible for shedding or shifting electric loads in the house, will receive the load control events and re-act based on the received events.

3.2.4.5 Zigbee and Security Concerns

The most concern in the Zigbee-based HAN network is the process of setting up a new device in the network and how the keys are established at both sides of the devices. When the new device is newly connected to the Zigbee network, the key must be established between the new device and its pair node. The key distribution for each pair of nodes in Zigbee standard can be done by three methods as follows:

---

[78] B. Gohn; Ember Cooperation, "Smart Meters and Home Automation", May 2008 [online]. Available: http://www.pointview.com/data/2008/05/22/pdf/Bob-Gohn-3024.pdf. [Accesses Jan 02, 2010]

- Provisioning or Commissioning is to use out-of-bound mechanism, such as pre-installation key or over-the-air key, to place the key into devices. The pre-install methods are not optimal because of the limitation of the ability to write the key in flash memory of the devices when changing the key. Also, the key is sent over-the-air in plaintext, which is susceptible to one-time eavesdropping attack. One way to help this issue is to ensure that devices are in close proximity.
- Key Transport is to have trust center distribute the keys to the devices. This method requires sending the key itself to the devices. The transportation of the key relies on the satisfactory security practice of the vendors. An attacker may be able to intercept the key, if the security mechanism for transporting the key is not secure enough to protect the key.
- Key Agreement is to have trust center and devices negotiate the keys without transport the key itself. According to R. Cragie[79], Key Agreement is the most secure method for key establishment between devices in the network. The key agreement is based on Symmetric Key Key Establishment (SKKE) which uses the master keys for distributing the shared secret key. However, the master key itself has the issue of the key distribution as well, since it has to be pre-installed or sent over-the-air.

Also, even though Zigbee supports security services and provide mechanism to defend against some attacks, such as eavesdropping and replay attacks, there is still the framework for exploiting IEEE 802.15.4 and Zigbee, called KillerBee. KillerBee framework is published by J. Wright[80], Senior Security Analysis at InGuardian Website in October 2009. It can be used to analyze Zigbee security; and could be used for Zigbee exploitation as well. KillerBee can be used for sniffing and injecting packets as well as decoding and manipulating network packets. The result[81] has shown some successful attacks using KillerBee to obtain the key and carry out replay attacks. If an attacker can inject the false message into the HAN network, the response of the device to the DR events or pricing information may be false. This can have financial and/or health-related impacts on homeowners. It also can lead to grid failure. Thus, using Zigbee alone may not be enough to provide security for Demand Response in HANs.

---

[79] R. Cragie, "Public Key Cryptographic in Zigbee Network", Dec 2008. [online]. Available: http://www.elektroniknet.de/fileadmin/user_upload/pdf/euzdc2008/Cragie_Jennic.pdf . [Accessed Jan 02, 2010]

[80] J. Wright; InGuardian, "An attack framework designed to explore vulnerabilities in ZigBee and wireless sensor networks", Oct 2009. [online]. Available: http://inguardians.com/pubs/toorcon11-wright.pdf. [Accessed Jan 03, 2010]

[81] J. Wright; InGuardian, "An attack framework designed to explore vulnerabilities in ZigBee and wireless sensor networks", Oct 2009. [online]. Available: http://inguardians.com/pubs/toorcon11-wright.pdf. [Accessed Jan 03, 2010]

3.2.4.6 *Zigbee and Security Measures*

Zigbee protocol is based on symmetric keys; the communication is secured by using shared key. However, the shared secret-key scheme has the issues in that if the key is compromised, all communications between the devices that use the same shared key will be no longer secure. Also, the key distribution is also expensive since Zigbee uses mesh-networking which means any device has to store the secret keys of all of its pair nodes in order to have multiple potential paths to route to their destination. Thus, symmetric algorithms cannot scale to a large system with hundreds of devices. The solution to these is to consider Elliptic-Curve Cryptography (ECC) as a public key scheme for Zigbee. ECC offers Elliptic-Curve Diffie-Hellman (ECCDH) key exchange which could be used for the key agreement method. According to NIST Recommendation for Key Management (Part 1)[82], ECC with 160-bit key provides equivalent encryption as strong as AES algorithm with 128-bit key. Also, authentication and non-repudiation can be provided by ECC as discussed in the section 2.3.3.

3.2.5 Demand Response Best Practices

To carry out load shed or load shift in buildings or residential areas, energy cost and control signals have to be sent via the Utility Gateway over a network, such as the Internet. When day-ahead and near real-time information arrive to an EMCS through the energy meter or gateway, the electricity demand will be moderated based on the signals received. A Home Area Network (HAN) will be used to distribute energy management information to all HAN devices in the building or home. All of the components used in DR programs, such as smart meters, HAN with DR capabilities, have potential vulnerabilities, once they are deployed on a network. An attacker may inject a malicious command into the system, collect personal information of the user, or modify the message contents. This section discusses best practices for DR systems in order to provide defend mechanisms against possible attacks specified in this chapter.

3.2.5.1 *Data Transmission*

To ensure integrity of the message, mutual authentication should be used between these devices. The DR and price signals and other information in the DR system also need to be encrypted in order to provide data confidentiality. The appropriate communication protocols for secure communication, such as Transport Layer Security (TLS) protocol, Internet Protocol Security (IPSec), Wireless Fidelity (WiFi) associated with IEEE 802.11i for a wireless local area network (WLAN) and IEEE 802.15.4 using ZigBee with elliptic curve cryptography (ECC) for sensor networks in HAN and NAN, can be used to protect network traffic.

3.2.5.2 *Data Handling Practices*

Information is sometimes sent between utilities and third party contractors, who may perform some kinds of collection of private data. Reusing and disclosing personal data by either utilities

---

[82] E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid; National Institution of Standard and Technologies (NIST), "Recommendation for Key Management – Part 1: General (revised)", March 08, 2007 [online]. Available: http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf

or third party could affect the privacy of customer information. Therefore, the information must be controlled in secure manners such that only necessary information of the customer is provided to any data collection entity and only authorized entities can access and use customer information. Also, the utility must obtain individual's permission prior to using personal information or disclosing private data to a third party. The length of time that a utility may retain customers' energy usage information must be specified. There are privacy issues which apply to other parts of the smart grid infrastructure. This will be discussed in more detail in the chapter on privacy issues of the smart grid.

3.2.5.3 Key Management

Key management is also critical in DR systems. Not only the information transmitted needs to be protected, but also the key itself needs to be authenticated and protected from the disclosure of the key to public. The use of X.509 public key certificate may provide such a protection.

3.2.6 Open Automated Demand Response (OpenADR) and Security Measures

This section uses the security concerns addressed in section 2.2 to derive security requirements and to provide some of the best practices based on the security requirements.

3.2.6.1 Security Requirements

The following set of general security requirements is derived from the security concerns specified in this chapter:

- All of the information transmitted in the OpenADR system must be protected from unauthorized access, inspection and modification from unintended users.
- Information transmitted either to or from the Demand Response Automated Server (DRAS) must maintain confidentiality and integrity from third parties.
- The DRAS must provide accountability for the following transactions
    - Prices received by participants
    - DR events received by participants
    - Bids submitted by participants
- The DRAS must maintain confidentiality of participants, utilities and ISOs.
- The proper access control to the information stored on the DRAS must be provided so that only authorized users can modify it.

3.2.6.2 Security Measures

The OpenADR communication is based on the Internet and Web Services technologies. Secure communication protocols, such as Transport Layer Security Protocol (TLS), can be used to secure network traffic. According to the OpenADR Communications Specification[83], the official

[83] M.A. Piette, G. Ghatikar, S. Kiliccote, E. Koch, D. Hennage, P. Palensky, and C. McParland, "Open Automated Demand Response Communications Specification", Demand Response Research Center,

TLS specification as published by the Internet Engineering Task Force (IETF) has been proposed as follows:

- 1024-bit Rivest, Samir & Adleman Public Key cryptography (RSA) for key exchange
- 3DES (Data Encryption Standard) and AES128 (Advance Encryption Standard) for data encryption
- SHA1 (Secure Hash Algorithm) for Message Integrity Code (MIC)
- Hashed MAC (HMAC) for Message Authentication Code.

According to this TLS specification, it is relatively safe and provides high-level integrity. However, TLS itself also has some vulnerability which will be described below. This section analyses those three approaches with respect to security issues mentioned above. (Note that at the time this chapter was being created, TLS version 1.1 and 1.2 has been released and RSA Laboratories has recommended it to use RSA with 2048-bit key in order to protect data beyond the year 2010[84])

The DRAS interfaces security can be implemented by three approaches as follows:

- TLS 1.0 with server-side certificates
- TLS 1.0 with server-side and client-side certificates
- Web Service Security (WS-Security)

1. TLS 1.0 with server-side certificates

This is most commonly employed in secure web servers. The server-side certificate is used for one-way authentication that allows clients to know that the web server which is responding to the request is the required one. The major flaw of this method is that the client is not authenticated which is subject to a number of serious Man-in-the-middle (MITM) attacks.

2. TLS 1.0 with server-side and client-side certificates

This approach is similar to the first one, but requires a client to provide its certificate for authentication. Even though, this mutual authentication provides the sense that client must be authenticated before communicating with the HTTPS servers, but the cost to implement this approach is extremely high since every clients' certificates need to be issued and maintained. In addition, there is a problem with TLS standard itself which is subject to MITM attacks related to renegotiation. TLS allows both server and client to request renegotiation, a new handshake that

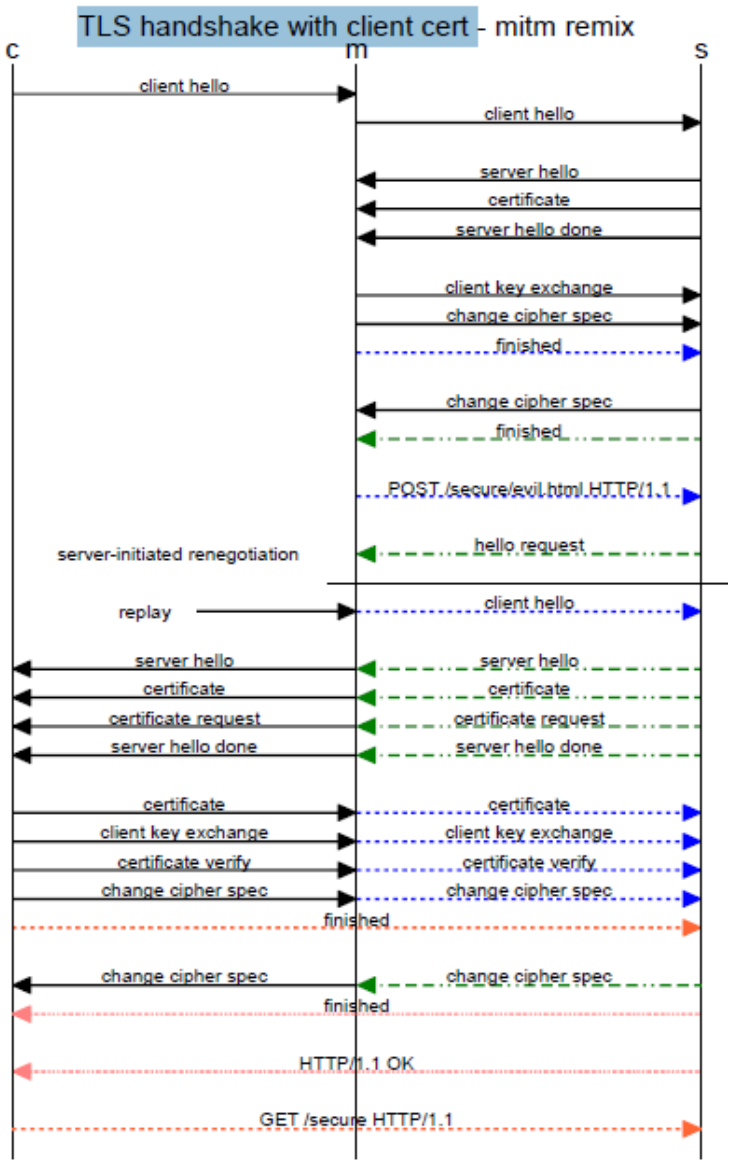
---

April 2009 [online]. Available: http://drrc.lbl.gov/openadr/pdf/cec-500-2009-063.pdf. [Accessed October 20, 2009]

[84] B. Kaliski, *"TWIRL and RSA Key Size"*, RSA Laboratories Technical Note, May 2003 [online]. Available: http://www.rsa.com/rsalabs/node.asp?id=2004. [Accessed Dec 05, 2009]

establishes new cryptographic perimeters, of the TLS session at any time. The problem is in order to obtain and validate the client certificate, the HTTPS server need to renegotiate the TLS channel. During the authentication, there is a loss of continuity, called “the authentication gap”, which occurs because there is no cryptographic binding between the old connection and the newly established one. The authentication gap bug in the TLS protocol allows an attacker to carry out a number of MITM attacks and inject data into the authenticated SSL communications. This demonstrates that the existing systems which are currently implemented using client certificates authentication are vulnerable. Figure 3-9 demonstrates the process of how an attacker can exploit the defect in TLS.

Figure 3-9: TLS handshake with client certificate and MITM attack85



The SSL/TLS renegotiation is vulnerable to a form of MITM attack, and hence to implement OpenADR all the SSL libraries need to be updated with the most recent patches. This vulnerability applies to SSL version 3.0, and all current versions of TLS (version 1.0, 1.1, and 1.2). Also, all the software which implements SSL communication is required to be updated with the latest vendor patches. The short-term fix of this problem is to not allow or disable

[85] M. Ray, S. Dispensa, PhoneFactor, Inc., "Renegotiation TLS version 1.1", Nov 4, 2009 [online]. Available: http://extendedsubset.com/?p=8. [Accessed Dec 3, 2009]

client-side certificates. However, this approach is intended to be used for more secure channel (which requires both server-side and client-side certificates). Thus, unless this vulnerability is fixed, this approach should not be used because the intended "more" security will not be realized.

IETF has defined a specification of a TLS extension which ties the re-negotiation to the TLS connection they are being operated which in turn fix this vulnerability. The details of the TLS extension could be found at RFC5746[86]. The status of vendor patches and updates on this SSL/TLS authentication gap could be found at PhoneFactor[87].

3. Web Service Security (WS-Security)

WS-Security is a specification for secure Web Services. It provides approach of how to enforce confidentiality and integrity on Web Services messaging. This standard includes the specification details of how to use Security Assertion Markup Language (SAML), Kerberos and Public Key Infrastructure (PKI) certificate format X.509. This section discusses how to enforce the security goals by using some of the cryptographic tools based on PKI and X.509 certificate format with WS-Security specification.

Encryption

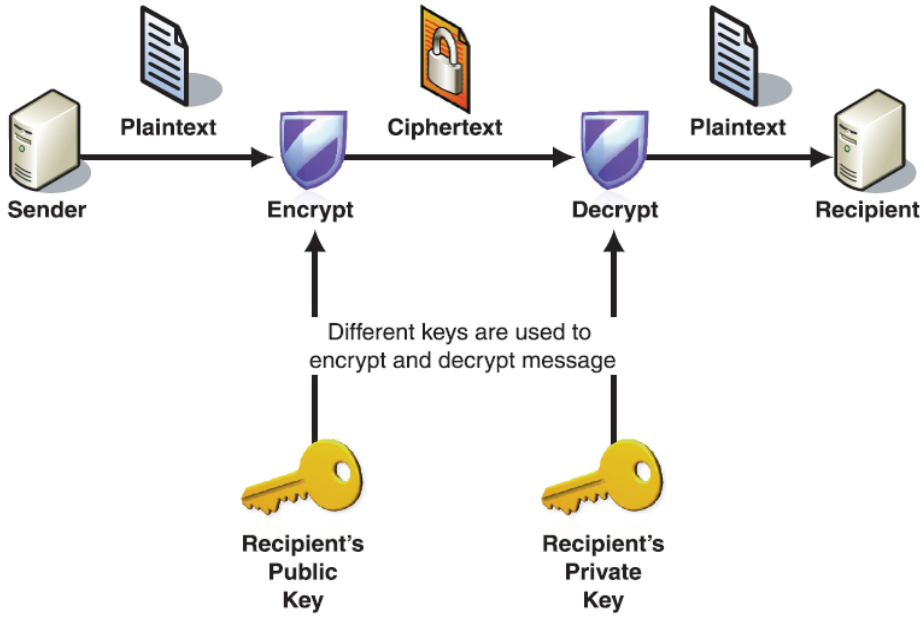
PKI supports both the encryption and signing. The use of encryption can be done by using the public key (Asymmetric Cryptography) from the X.509 certificate issued by the CA in order to provide data confidentiality. Figure 3-10 below shows the use of public key encryption.

---

[86] E. Rescorla; RTFM, Inc., M. Ray, S. Dispensa; PhoneFactor, N. Oskov; Microsoft, "Transport Layer Security (TLS) Renegotiation Indication Extension", Internet Engineering Task Force (IETF), Request for Comments(RFC) 5746, February 2010 [online] Available: http://www.rfc-editor.org/rfc/rfc5746.txt

[87] PhoneFactor, "Status of Patches for SSL/TLS Authentication Gap" [online] Available: http://www.phonefactor.com/sslgap/ssl-tls-authentication-patches

Figure 3-10: Asymmetric Cryptography88



However, in the OpenADR system, the information can be real-time based, such as Real-time pricing signal. Using public key encryption could be slow due to the size of ciphertext. Another approach is the combination of both symmetric and asymmetric cryptographies. The public key can be used as a long-term key and symmetric key can be used as a short-term or one-time key. The public key is used to establish a temporary shared secret key between the communication pairs by encrypting the shared key and negotiate with the client. After the shared key is established, both communication pairs use this key to encrypt and decrypt messages.

There are some security issues in providing data confidentiality that need to be addressed.

1. Given the same plaintext, the ciphertext should never be repeated. Randomness can be used to attach with the message, so that the encrypted message will never be repeated.
2. Ciphertext should never be used by an eavesdropper to replay the message. Time stamping can be used to validate that the message is a replay.
3. Encrypted message should never differ in length.

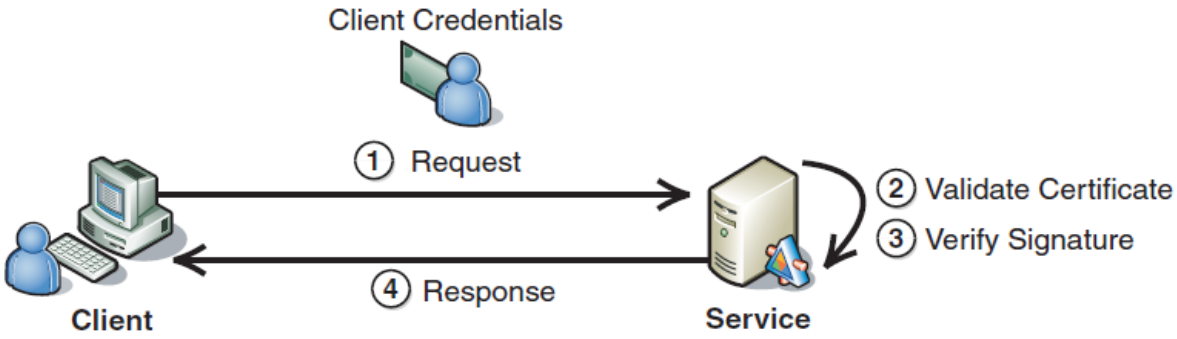
Source Authentication

---

[88] Microsoft Developer Network (MSDN) library, Microsoft Corporation, "Web Service Security Scenarios, Patterns, and Implementation Guidance for Web Services Enhancements (WSE) 3.0", 2009 [online]. Available: http://msdn.microsoft.com/en-us/library/aa480545.aspx. [Accessed Dec 4, 2009]

In order to implement authentication with X.509 certificate, Certificate Authority (CA) and Certificate Store are needed. The certificate store is the place where all the X.509 certificates are stored. The X.509 certificates issued by the trusted CA are used to verify that the identity of both the server and client are valid. The certificate includes the credentials, such as the identity and public key, and the signature part which is produced by signing the message with the private key of the CA. When the server received the message, it will use client's public key obtained from the X.509 certificate to validate the signature. The server ensures that the message came from the claimed source and that the X.509 certificate has not expired.

Figure 3-11: Authentication using X.509 certificate[89]



Message Authentication

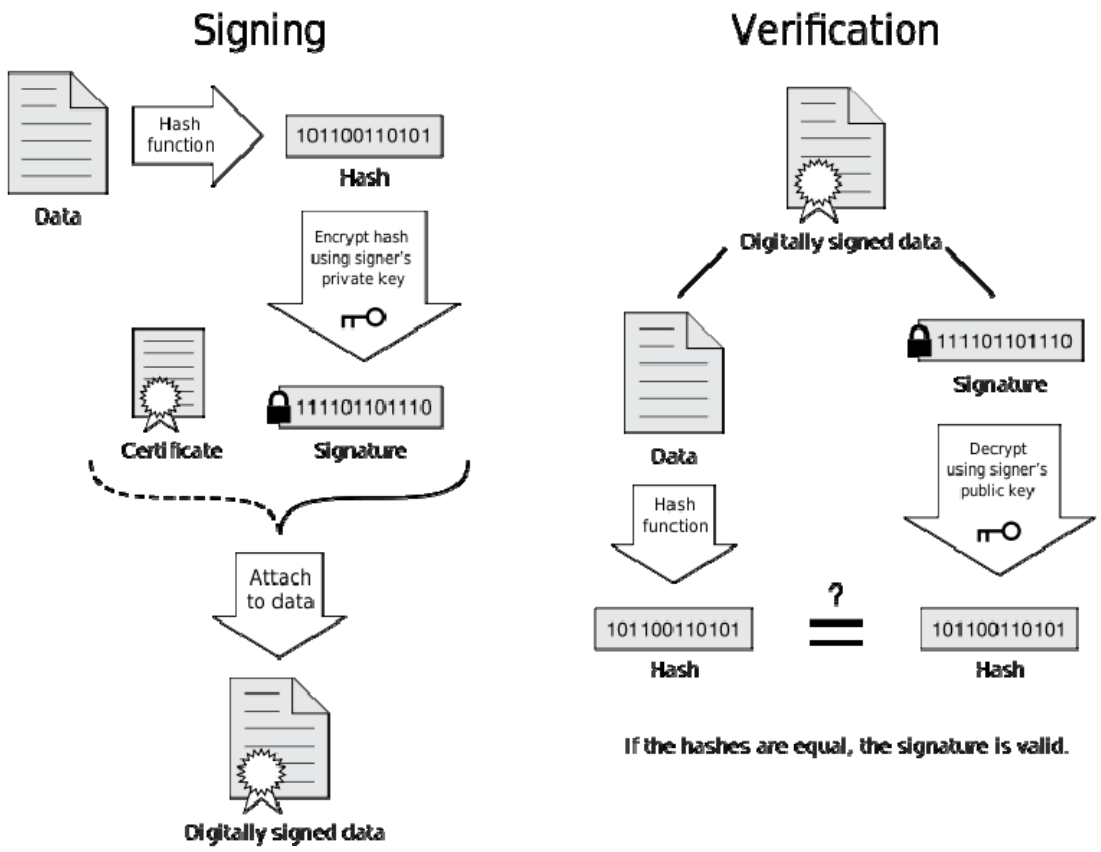
Encryption does not necessarily provide protection from unauthorized modification of the message. Thus, message authentication is needed to provide data integrity. The most commonly used technique is to use Digital Signature Algorithm (DSA) in conjunction with RSA algorithm. Signature is generated by using the sender's private key and an appropriate Secure Hash Standard (SHS) which should comply with the Digital Signature Standard (DSS), FIPS PUB 186[90], from the National Institute of Standards and Technology (NIST). The verification process is done by using the corresponding public key of the sender and the same hash function. The receiver of the message can ensure that the message came from the source that it claims and the message is not tempered with by anyone because the only corresponding public key and the same hash function can verify the signature part and only the user that possesses the private key can digitally sign the message. Figure 3-12 demonstrates the process of signing and verification using Digital Signature.

---

[89] Microsoft Developer Network (MSDN) library, Microsoft Corporation, "Web Service Security Scenarios, Patterns, and Implementation Guidance for Web Services Enhancements (WSE) 3.0", 2009 [online]. Available: http://msdn.microsoft.com/en-us/library/aa480545.aspx. [Accessed Dec 4, 2009]

[90] Digital Signature Standard is available at http://www.itl.nist.gov/fipspubs/fip186.htm

Figure 3-12: The signing and verification process of Digital Signature91



Non-repudiation

Non-repudiation can be provided by using the digital signature technique. Typically, the private key is only known by the owner and restricted from public. Thus, using the corresponding public key can ensure that the sender is the only one who signed the message.

Key Pair Management

The key management is one of the critical parts of OpenADR. A best practice is to use different key pairs for encryption and digital signature since the signatures are used for longer-term authentication and message integrity, but the encryptions are done by using a shorter-term key pair. Also, the key distribution, revocation and key backup processes tend to be different based on what the keys are used for. For example, if the encrypted message is store on hard disk, the archived version of the private key may be needed to decrypt the encrypted message.

---

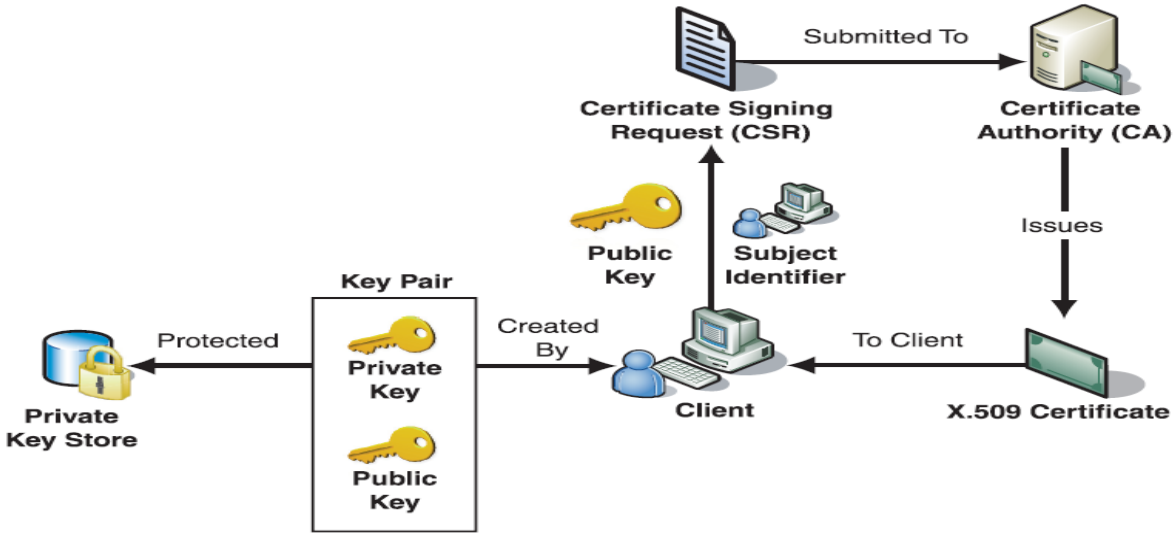
[91] Wikipedia, "Digital Signature", Nov 2009 [online]. Available: http://en.wikipedia.org/wiki/Digital_signature [Accessed Dec 3, 2009]

Nevertheless, the key pair for digital signature may not need to be changed. Also, to protect a public and private key pair, the secure place to store the private key is needed and it should be restricted such that only an authorized party can access it. Typically, the private key should not be accessed by or sent to any other party including the CA. The public key is needed to be protected from unauthorized modification as well. The public keys from X.509 certificates are signed by the trusted CA which can provide such the protection.

Certificate Management

Certificate management depends on the type of CAs which can be an internal or external organization. For the external CAs, X.509 certificates can be simply obtained by submitting a certificate signing request (CSR). The public/private key pairs will be generated only for use with the requested certificate. For the internal CAs, the certificate management varies depending on to the organization. However, CSR can be used for obtaining the certificates as well. Figure 3-13 shows the process of a client requesting an X.509 certificate from a CA that processes CSR and the process of a CA issuing an X.509 certificate.

Figure 3-13: Requesting and obtaining process for X.509 certificate92



If the integrity of the certificate has been compromised, the CA has to revoke X.509 certificates. The certificate revocation list (CRL) is typically available to the public, so that any recipients of a signed message can verify that the certificate has not been revoked.

---

[92] Microsoft Developer Network (MSDN) library, Microsoft Corporation, "Web Service Security Scenarios, Patterns, and Implementation Guidance for Web Services Enhancements (WSE) 3.0", 2009 [online]. Available: http://msdn.microsoft.com/en-us/library/aa480545.aspx. [Accessed Dec 4, 2009]

Security Consideration in Implementation of X.509 Certificate with WS-Security

In OpenADR systems, security concerns are focused on confidentiality and both source and data integrity. X.509 certificates can be used as a binary security tokens with the WS-Security specification defined in the OASIS standard for SOAP message security[93] in order to provide confidentiality and integrity of the message. In WS-Security, message integrity can be provided by using XML signature in conjunction with X.509 certificates. Also, to keep SOAP (Simple Object Access Protocol) message confidential, XML encryption also can be used in conjunction with X.509 certificates. Even though, using X.509 certificate can reduce the risks of MITM attacks, the designer should be aware that using digital signature alone may not be sufficient to secure SOAP messages. A replay attack could be carried out, if there is no mechanism to detect it. Time stamp, sequence number or expiration date can be included into the signature part of the message or of the SOAP header for some SOAP extension. The use of WS-Security in conjunction with X.509 certificates provides a great deal of flexibility and high-level of confidentiality and integrity, but it tends to have some impacts on the system performance, such as speed and complex computation.

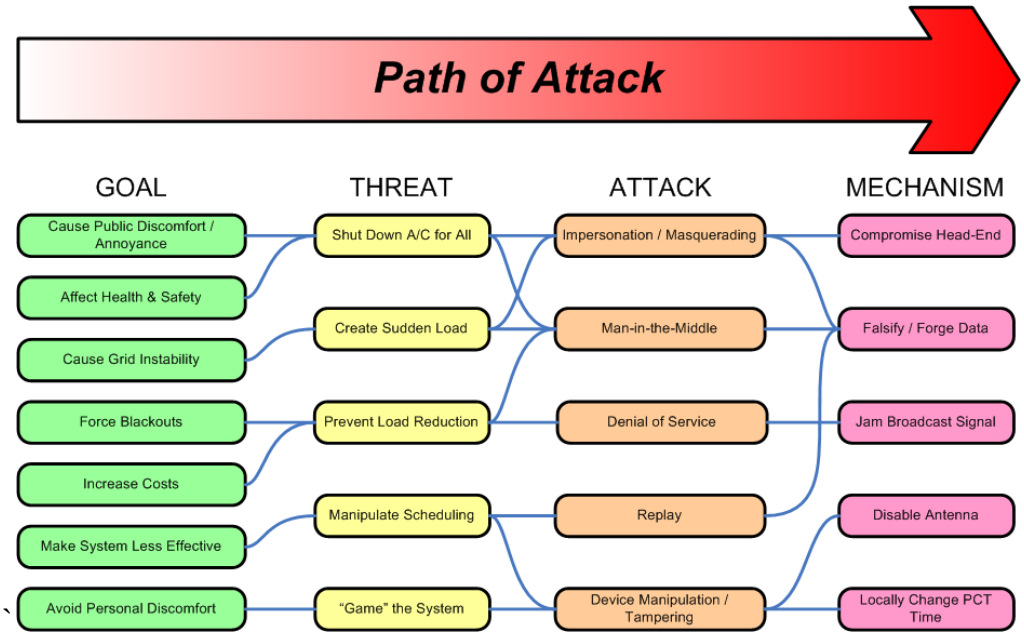
3.2.6.3 Demand Response at Residential Sites and Security Concerns

The demand response for residential customers is carried out by using a Programmable Communicating Thermostat (PCT). PCT Communication takes place through a broadcast wireless network, such as sub carrier FM, which allows large number of PCTs to receive the information in a single broadcast transmission. When the DRAS receives the demand response signals from the utility, it will provide the signals to a network operating center (NOC), which is responsible for the broadcast of the signals to PCTs. Broadcast messages, consisting of the price signal, will be sent out to the thermostat in order to update the power consumption at the residential sites. The broadcast messages could be manipulated by an adversary in such a way that they can affect the energy usage in residential areas. For example, an attacker may attempt to turn on all air-conditioning units in the residential site resulting in excessive loads to the grid, and blackouts may occur. Also, an attacker could send false message which is not issued from the broadcast network, causing incorrect response from the PCT and incorrect energy price is set. Figure 3-14 summarizes goals of an adversary, threats, possible attacks and mechanism for each scenario on the PCT systems.

---

[93] A. Nadalin, IBM Corporatation; C. Kaler, Microsoft Corporation; P. Hallam-Baker, VeriSign Inc.; R. Monzillo, Sun Microsystems Inc., "Web Services Security: SOAP Message Security 1.0 (WS-Security 2004) OASIS Standard 200401", March 2004 [online]. Available: http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf. [Accessed Dec 4, 2009]

Figure 3-14: Path of Attack in PCT System94

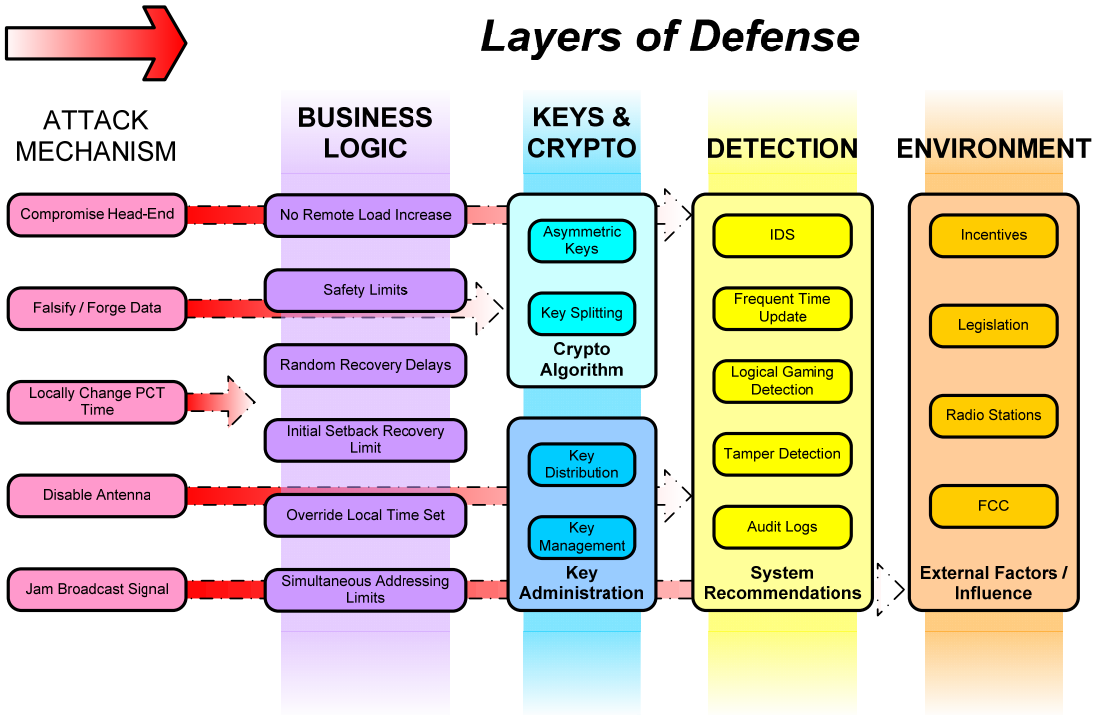


3.2.6.4 Demand Response at Residential Sites and Security Measures

To defend against the security concerns discussed in the section 3.2.5.3, the layer of defense has been addressed as shown in Figure 3-15.

[94]E. W. Gunther, "Reference Design for Programmable Communicating Thermostats Compliant with Title 24-2008", March 2007 [online]. Available: http://drrc.lbl.gov/pct/docs/ReferenceDesignTitle24PC_rev15.doc. [Accessed October 22, 2009]

Figure 3-15: Defend Mechanisms for PCT systems95



This section focuses on the use of cryptographic approaches to provide defensive mechanisms against the security concerns since they are considered as the main defense against attacks. The further details of business logic, detection and environment layers are in the Reference Design for PCT[96].

Cryptographic Approaches

E. W. Gunther[97] has recommended using Elliptic Curve Cryptography (ECC), which is based on the asymmetric approaches and consumes low energy. The use of ECC for authentication and confidentiality is already discussed in section 3.2.2.6.

---

[95]E. W. Gunther, "Reference Design for Programmable Communicating Thermostats Compliant with Title 24-2008", March 2007 [online]. Available: http://drrc.lbl.gov/pct/docs/ReferenceDesignTitle24PC_rev15.doc. [Accessed October 22, 2009]

[96]E. W. Gunther, "Reference Design for Programmable Communicating Thermostats Compliant with Title 24-2008", March 2007 [online]. Available: http://drrc.lbl.gov/pct/docs/ReferenceDesignTitle24PC_rev15.doc. [Accessed October 22, 2009]

[97] E. W. Gunther, "Reference Design for Programmable Communicating Thermostats Compliant with Title 24-2008", March 2007 [online]. Available: http://drrc.lbl.gov/pct/docs/ReferenceDesignTitle24PC_rev15.doc. [Accessed October 22, 2009]

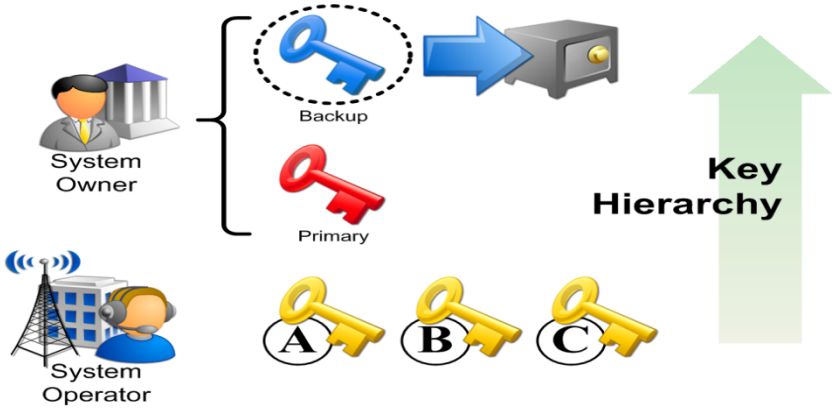
Key Distribution

The challenge in the case of PCT is the key distribution issues. When the PCT devices are manufactured, the unique random number must be place into each PCT. This number will be used in the installation process as well as the transmission of cryptographic key information to the device. The key materials could be embedded into the device. This may lead to the issue of key handling and storage since if the PCT is stolen, the knowledge of the key information might be leaked. One solution to this is to separate critical information, such as the key, so that there must not be any single entity possessing enough information by itself to reconstruct the secret. In the PCT system, the random number could be placed into the thermostat along with an out-of-band communication channel. The out-of-band channel could be a phone number or activation code which the installer of the PCT could obtain it confidentially in order to activate or install the PCT into a residential site.

Key Management

Key management for PCT system utilizes a three-tiered hierarchy of keys as shown in the figure 3-16.

Figure 3-16: Hierarchy of the Key Distribution98



The benefit of the hierarchy is that when the primary key is compromised at some point, the backup key can be used instead. The backup key will never be used and keep in secure storage, if the primary one is not compromised. In this hierarchy, there are two entities which are system owner and system operator.

System Owner is the highest level of authority for overseeing and control of the entire PCT system. Any Information transferred from the System Owner to the PCT must go to the System Operator. The system owner possesses two separate public/private key pairs, one primary and

---

[98] E. W. Gunther, "Reference Design for Programmable Communicating Thermostats Compliant with Title 24-2008", March 2007 [online]. Available: http://drrc.lbl.gov/pct/docs/ReferenceDesignTitle24PC_rev15.doc. [Accessed October 22, 2009].

one back up keys. The primary keys will be used when the system owner authenticates the public key of the system operator and also when the system owner sends system-wide messages, such as emergency messages.

System Operator is the responsible for sending messages to PCTs. A public/private key pair will be used for all PCT communication from system operator to PCTs. In some case, the system operator may possess more than one key pair based on the different operating regions, or service territories.

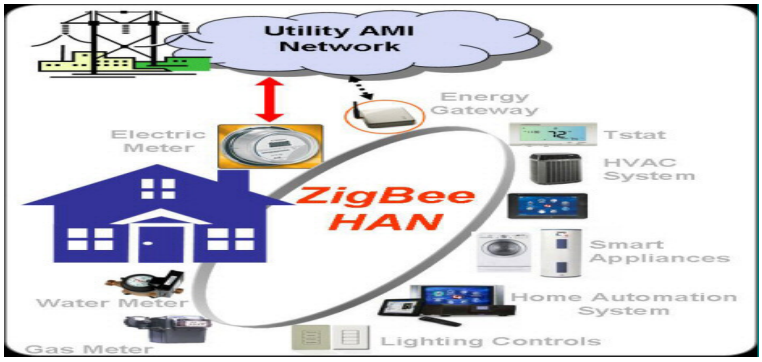
3.3 Customer Domain – Home Area Network, Gateway, Neighborhood Area Network

3.3.1 Introduction

The customer domain consists of a Neighborhood Area Network connecting the utility to the smart meter installed in the homes of the consumer, the gateway and finally the Home Area network which connects all the appliances at home. There were several security concerns raised within each of the domains and the respective potential security threats were addressed.

In the following sections we will be discussing best practices to overcome these security loopholes within each area of communication.

Figure 3-17: Customer Domain which includes WNAN, gateway and HAN99



3.3.2 Neighborhood Area Network

In Smart Grid, wireless neighborhood area network (WNAN) has a role to play in the HOME-to-HOME or HOME-to-GRID communication. The WNAN coverage range extends anywhere from the coverage of wireless local area network (WLAN), to wireless wide area network (WWAN). The potential threats, issues and vulnerabilities associated with the protocols considered for WNAN are briefly summarized below.

[99] http://www.sensorsmag.com/files/sensor/nodes/2008/1526/Figure2.jpg

3.3.2.1 IEEE 802.11

Wireless network is available everywhere and the attacker need not be in close proximity to the victim. Management frames are not authenticated hence the attacker can take advantage and redirect the traffic and can also corrupt the ARP tables. DOS attacks are performed by introducing the noise into the network. Without proper employment of encryption techniques, there is a scope for eavesdropping and manipulating.

The following are the observed problems with wireless local area network (WLAN) as shown in chapter 2:

- Convenient Access
- Rouge Access Points
- MAC Spoofing
- Denial of Service attacks
- Man-in-the-middle attacks

3.3.2.2 IEEE 802.15.4

Encryption scheme must be used to prevent message recovery. To avoid semantic security violation, unique nonce values are used while encryption. The same nonce is sent in the packet with encrypted data and hence decryption is not dependent on the nonce affecting confidentiality. The ACL table gets cleared in case of power failure there by resetting the nonce to known values and hence the reuse of nonce is incurred, compromising the security. The inability of ACL tables to support different keying modes like group keying and network shared keying could lead to reply attacks. These replay attacks could result in rejecting packets thereby causing denial of service.

The following are the observed problems with IEEE 802.15.4 protocol as shown in chapter 2:

- Confidentiality
- Loss of ACL State
- Key Management Problems
- Confidentiality and Integrity Protection
- Denial of Service
- No Acknowledgment Packet Integrity

3.3.2.3 IEEE 802.16

Wimax is prone to man-in-the-middle attacks, exposing customers to confidentiality and availability attacks as there is no base station authentication schema. Management frames are not encrypted and hence information about subscribers in the area and also about network characteristics could be obtained but an attacker. An attacker can also send a series of frames to a node to drain the battery life.

The following are the observed problems with IEEE 802.16 protocol as shown in chapter 2:

- Authentication

- Encryption
- Availability
- Water Torture Attacks

3.3.3 Best Practices for WNAN

3.3.3.1 IEEE 802.11

The following section describes the recommendations for the security of 802.11 networks:

1. **Media access control (MAC) address filtering**[100] would allow us to configure our wireless access points (APs) with the set of MAC addresses for allowed wireless clients.

Pros: Helps receive information from authentic sources and prevents unauthorized access.

Cons: Does not prevent a hacker from MAC spoofing, increases administrative overheads.

2. **Wi-Fi Protected Access (WPA)** has an improved encryption algorithm called Temporal Key Integrity Protocol (TKIP) which uses a unique key for every client and also uses longer keys that are rotated at configurable intervals. WPA also includes an encrypted message integrity check field in the packet to prevent denial-of-service and spoofing attacks.

Pros: With the use of WPA2, VPN connections are not required to secure the wireless frames.

3. **IEEE 802.11w-2009**[101]: The management information is sent in unprotected frames, which cause network disruption by malicious systems that forge disassociation requests that appear to be sent by valid equipment. IEEE 802.11w-2009 is an approved amendment to IEEE 802.11 to increase security of the management frames. The objective of this protocol is to increase the security by providing data confidentiality of management frames, mechanisms that enable data integrity, data origin authenticity, and replay protection.

3.3.3.2 IEEE 802.15.4

The following section describes the recommendations for the security of 802.15.4 networks:

1. **MAC address filtering**: This security mechanism is defined with the IEEE 802.15.4 standard and is defined in the Access Control List (ACL) mode. This feature should be enabled to accept the received MAC frames from authorized nodes listed in the ACL for the host device.
2. **Flash memories**: The loss of ACL entries during power failure or low powered operation could be fixed by saving and storing the nonce states in flash memories. But the use of such flash memories incur an additional cost, power consumption and also is slow and energy inefficient.
3. **AES encryption standards**[102]: Data privacy protection mechanisms based on AES encryption

---

[100]http://technet.microsoft.com/en-us/library/bb457091.aspx

[101]Wikipedia http://en.wikipedia.org/wiki/IEEE_802.11w-2009

[102] Ken Masica, Recommended Practices Guide for Securing Zigbee Wireless Networks in Process Control System Environments. Draft version. Lawrence Livermore National Laboratory. April 2007.

standard should be used to protect the transmitted data.

4. **Source node authentication:** A concept similar to shared secret key or unique session key that is derived between two entities in order to secure data transmitted between them should be used to implement source node authentication.

3.3.3.3 IEEE 802.16

The following section describes the recommendations for the security of 802.16 networks:

1. **Message Authentication Code (MAC) techniques**[103]**:** For vulnerability of management message, message authentication code techniques can be applied during initial ranging. For example, one-key message authentication code (OMAC) may be preferable since it provides replay protection

2. **Protection against masquerading parties:** A mutual authentication scheme is necessary, and Extensible Authentication Protocol (EAP), a generic authentication protocol used in wireless networks, is most commonly proposed.

3. **AES-CCM5:** AES in CCM mode constructs a unique nonce during the process of CBC-MAC. AES-CCM also has an advantage that the encryption scheme is also capable to protect authenticated but unencrypted data.

3.3.4 Gateway

The home gateway component is an integral part of the customer domain architecture. Since it connects a varied Standard home area network to a native AMI communication standard, it needs to act as negotiation agent and also it needs to do the function of a translation unit. If the gateway is compromised then it could harm either the utility or the home appliances or at times both. Considering the significance of this component the need to come up with a secure solution is at its prime. We in this chapter, discuss some of the possible countermeasures to the security problems mentioned below.

3.3.4.1 Best Practices for Gateway

1. **MAC address filtering:** When a new gateway is added to the network it would send out its MAC as identification to the utilities. These MAC addresses have to be entered in the Access Control List (ACL) of all intermediate hubs to prevent the MAC address spoofing. But the downside to this approach is once the valid MAC address is sniffed then it can be used to access the network. To avoid eavesdropping we would require using of an encryption scheme.

2. **Low Power Encryption techniques**[104]**:** The use of low power cryptographic schemes like the Asynchronous VLSI implementations of International Data Encryption Algorithm (IDEA). This approach proves to be the most efficient in terms of power consumptions.

3. **Central Authority for Public Key Infrastructure:** The need of a central certifying authority in such set up cannot be more emphasized. The central authority would not just be a certificate issuing unit, but also a central regulatory board which would control all the software and

---

[103] Hyung-Joon Kim, IEEE 802.16/WiMax Security, Stevens Institute of Technology, Hoboken, New Jersey

[104] P Kitsos, O Koufopavlou, G Selimis and N Sklavos , Low Power Cryptography, VLSI Design Lab, Electrical and Computer Engineering Department, University of Patras.

hardware updates to the critical components of the Smartgrid.

4. **Trusted Platform Module**[105]**:** In computing, Trusted Platform Module (TPM) is the name of a published specification detailing a secure crypto processor that can store cryptographic keys. The TPM can be used to store the Public and Private Key pairs in the sealed storage.

5. **Virtual Home**[106]**:** The use of a virtual home is beneficial from the consumer's perceptive; since gateway incorporates a virtual home set up which would execute all the commands received from the outside world on itself before deploying it on the real environment. This adds a security shield to the home area network, but since operation of this virtual home is vital the software updates and hardware tampering needs to be controlled by the regulatory board.

3.3.5 Home Area Network

Home area network is last link in the chain connecting utility to the customer. Since it resides in such close proximity of the consumer, a security failure would directly affect lives of the end user. The Home Area Network (HAN) protocol considered here is ZigBee and security loopholes within the protocol has been discussed in the chapter Smart grid cyber security potential threats, vulnerabilities and risks. In this chapter, we would be considering best practices for Zigbee and suggesting counter measures for the security threats.

ZigBee: ZigBee's protocol stack is structured in layers. The physical and the media access layer are based on the IEEE 802.15.4 standard. IEEE 802.15.4 is a standard which specifies the physical layer and media access control for low-rate wireless personal area networks. It focuses on low-cost, low-speed ubiquitous communication between devices. The 2 layers on top of this stack is ZigBee specific which is General Operation Framework and the Application layer.

Using of Flash memory: The threat scenario due to power failure can be resolved by storing nonce states in flash memory which incurs additional cost, power consumption and energy inefficient.

Avoiding Counter mode in AES: To overcome fast Denial-Of-Service attack, we can avoid using the counter mode in the AES (Advanced Encryption Standard) and use other modes such as CCM which is counter with CBC-MAC (Cipher Block Chaining Messages Authentication Code).

Using Single Access Control List (ACL): There is no support for using the same keys for multiple ACL entries. Since ZigBee allows this there is problem of nonce states being reused. To fix the problem we could create a single ACL entry for a particular key. Before sending, changing the destination address associated with that ACL entry for a message would suffice to fix this issue.

---

105 http://en.wikipedia.org/wiki/Trusted_Platform_Module

106 Khusvinder Gill, Shuang-Hua Yang, Fang Yao, and Xin Lu A ZigBee-Based Home Automation System. Loughborough University, UK 2009.

3.3.5.1 General Best Practices for ZigBee[107]

The following are recommended practices that should be considered when implementing a ZigBee LR-WPAN network:

- **Creating a Security Policy within the organization:** Develop a general LR-WPAN technology security policy and make it part of the existing IT policy would help authorize the use of LR-WPAN networks within the organization and specify the roles and responsibilities of personnel to ensure their safe and secure operation.
- **MAC Address Filtering:** This is the security mechanism defined with the IEEE 802.15.4 standard and is the Access Control List (ACL) mode. This feature should be enabled to accept received MAC frames from authorized nodes listed in the ACL for the device.
- **Encryption:** To protect the transmitted data ZigBee provides data privacy protection mechanism based on AES encryption standard.
- **Source node authentication:** A destination node in a ZigBee network can use a link key derived from their respective master keys to verify the identity of the source device. The link key is unique for a pair of devices that communicate with each other. (This is equivalent to the concept of a unique session key that is derived between two entities in order secure data transmitted between them.)
- **ZigBee Coordinator:** ZigBee coordinator is a node that is responsible for initiating the formation of network, sending the beacon transmissions and setting the security level. Unlike in Bluetooth where there is only one fully functional device (FFD) and the rest are reduced functional devices (RFD), ZigBee could have more than one fully functional device and hence it becomes important to designate a ZigBee coordinator for the network, which owns the responsibility to perform the above-mentioned essential functions. It is also advisable to have a backup ZigBee coordinator which comes handy in case of failure.
- **Restrict node connectivity using a pre-assigned PAN Identifier:** If multiple ZigBee networks are operating in a given environment there is a high possibility for conflicts to occur. Hence a ZigBee network policy could be employed to use the permit join access control to restrict device connectivity. This is performed in addition to configuring a dedicated ZigBee Coordinator for the network, where in ZigBee nodes should be limited to joining only the network with the pre-assigned PAN Identifier.
- **Out-of-band key loading method:** This is one of the possible key management methods used by ZigBee vendors. In this method the key could be loaded on the device using methods other than the normal wireless communication channels like, via a serial port of the device connected to a key generation device like a laptop or trust center.
- **Secure network admission control:** The secure join method provides a way to authenticate the nodes requesting admission and decide whether or not to permit the

[107]Ken Masica, Recommended Practices Guide for Securing Zigbee Wireless Networks in Process Control System Environments. Draft version. Lawrence Livermore National Laboratory. April 2007.

node to join the network. This functionality is carried out by a ZigBee Trust Center where in it allows nodes to first associate themselves to a network and then authenticates to it. This is done by pre-loading a common network shared key in the devices before deployment.

- **Trust Center address to be preconfigured in all nodes:** The Trust Center (TC) is the central element in the ZigBee security architecture and is trusted by all devices in the network. The address of the TC should be pre-loaded into the ZigBee node.
- Interference: Industrial environments can produce a significant amount of electromagnetic noise from machinery such as pumps, motors, fans, and various actuator devices, thereby reducing the signal-to-noise quality of transmissions in a LR-WPAN network. The MAC layer of 802.15.4 is based on the CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) channel access method in which a station will first listen or an open channel before transmitting. This is done by sensing the energy level in the frequency band corresponding to the channel. The possible solution to over this interference problem include:
    - Choosing the least susceptible 802.15.4 frequency band (900MHz or 2.4GHz) for a given industrial environment.
    - Configuring the ZigBee devices to use a particular channel within the selected frequency band that is least affected by the EMI.
    - Increasing the transmit power level of the ZigBee devices by selecting a product that supports higher power levels or using a higher-gain antenna.
    - Deploying a mesh topology to allow a ZigBee device to have multiple next-hop neighbors to communicate with and therefore *spatial diversity* in terms of multiple transmission paths. Higher node density will also permit shorter distances between ZigBee devices and can result in increased received signal strength and improved signal-to-noise ratios.
    - Using a Frequency Hopping (FH) radio with configurable hopping channels and patterns. This type of temporal and frequency diversity approach can improve EMI immunity in an industrial environment as well as provide an additional measure of security if a non-default hopping pattern is used and also changed on a periodic basis.

3.3.6 Comprehensive Best practices for securities with HAN/Gateway/ WNAN

Table 3-18: Comprehensive Best practices for securities with HAN/Gateway/ WNAN

Component Involved	Threat Scenario Description	Best Practices
U-SNAP	MAC address spoofing Public Key Infrastructure security issues	MAC address filtering Low Power Cryptography techniques Central Authority for Public Key Infrastructure

Component Involved	Threat Scenario Description	Best Practices
ZigBee Gateway Module	External security threats and loopholes	Virtual Home
ZigBee	Power Failures Fast Denial-Of-Service Attack on AES-CTR Allows the use of Same Keys on multiple ACL entries	Using of Flash memory Avoiding Counter mode in AES Using Single Access Control List (ACL)
IEEE 802.11	MAC Spoofing Denial of Service Attacks Man-in-the-Middle Attacks	Media access control (MAC) address filtering Wi-Fi Protected Access (WPA) IEEE 802.11w-2009
IEEE 802.16	Authentication Encryption Availability Water Torture Attack	Message Authentication Code (MAC) techniques Protection against masquerading parties AES-CCM
IEEE 802.15.4	Confidentiality Loss of ACL State Key Management Problems Confidentiality and Integrity Protection Denial Of Service No Acknowledgment Packet Integrity	MAC address filtering, AES encryption standards Flash memories AES encryption standards Source node authentication

3.4 Advanced Metering Infrastructure (AMI)

3.4.1 Introduction

Advanced Metering Infrastructure (AMI) refers to systems that measure, collect and analyze energy usage, from advanced devices such as electricity meters, gas meters, and/or water meters, through various communication media on request or on a pre-defined schedule. This infrastructure includes hardware, software, communications, customer associated systems and meter data management (MDM) software.[108]

The network between the measurement devices and business systems allows collection and distribution of information to customers, suppliers, utility companies and service providers.

[108] Wikipedia; Advanced Metering Infrastructure; Available [Online]: http://en.wikipedia.org/wiki/Advanced_Metering_Infrastructure

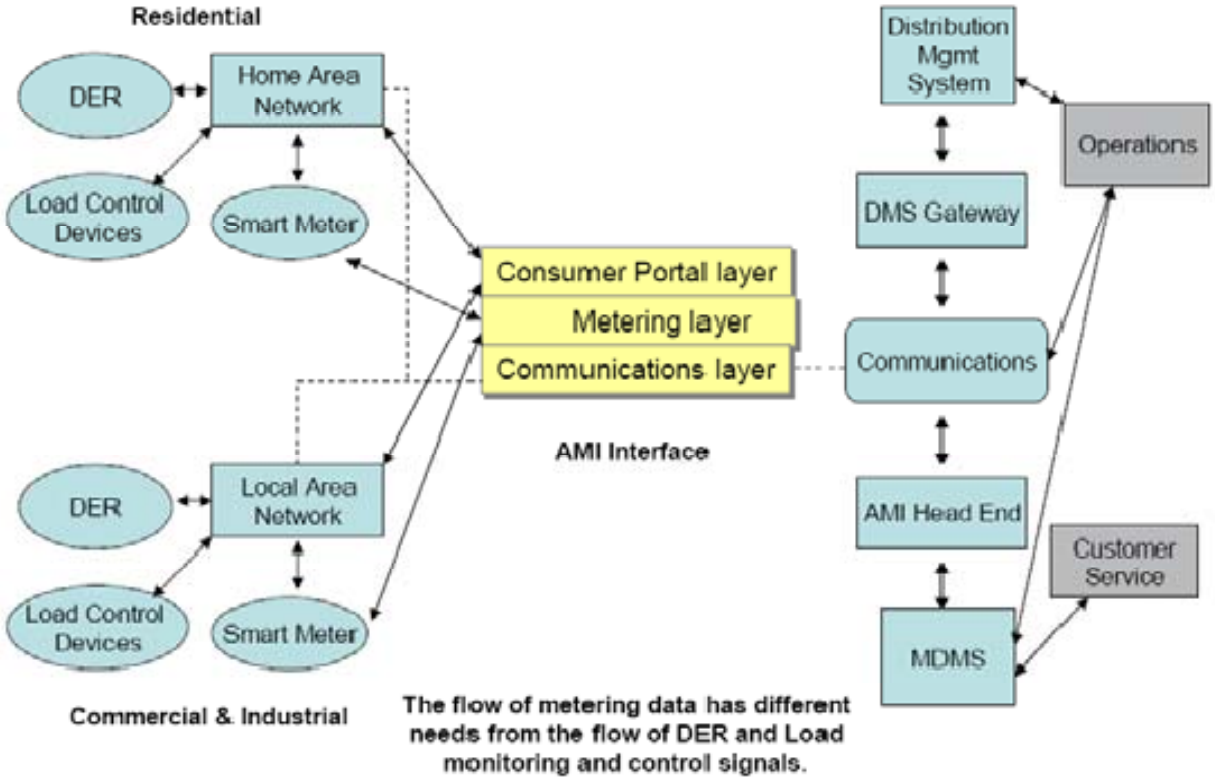
This enables these businesses to either participate in, or provide, demand response solutions, products and services. By providing information to customers, the system assists a change in energy usage from their normal consumption patterns, either in response to changes in price or as incentives designed to encourage lower energy usage use at times of peak-demand periods or higher wholesale prices or during periods of low operational systems reliability.

AMI systems are viewed as consisting of the following components (see also Figure 3-17):[109]

- Smart Meter – The smart meter is the source of metrological data as well as other energy-related information. These smart meters can provide interval data for customer loads as well as distributed generation.
- Customer Gateway – The customer gateway acts as an interface between the AMI network and customer systems and appliances within the customer facilities, such as a Home Area Network (HAN) or Building Management System (BMS). It may or may not co-locate with the smart meter.
- AMI Communications Network – This network provides a path for information to flow from the meter to the AMI head end.
- AMI Head End – This system manages the information exchanges between external systems, such as the Meter Data Management (MDM) system and the AMI network.

[109] Open Smart Grid; Shared Documents; Available [Online]: http://osgug.ucaiug.org/Shared%20Documents/Forms/AllItems.aspx

Figure 3-18: AMI Components



Source: Open Smart Grid; Shared Documents;[110]

111

3.4.2 AMI Security best practices [111]

Utilities are spending considerable amount of resources to develop Advance Metering Infrastructure systems with future vision that provides operational efficiency by enabling consumers to participate in personal energy management and conservation and also supports smart energy, distribution grids etc.

AMI have several benefits including filed operations, load forecasting, meter management and several areas such as: customer care, power outage management, reducing dependence on nonrenewable resources lowering exposure to spot market energy pricing and moderating greenhouse gas emissions. Further, it also covers consumer benefits such as: allowing utilities the ability to provide consumers with real-time energy monitoring and Demand Response programs, dynamic energy pricing and new energy management services. Thus, consumer saves money on their bills.

---

[110] Open SG User Groups. http://osgug.ucaiug.org/Shared%20Documents/Forms/AllItems.aspx.

[111] Critical Infrastructure Protection for AMI Using a Comprehensive Security Platform: http://certicomcenterofexcellence.com/pdf/white_paperami_advanced_metering_infrastructure.pdf

As, technology progresses, it comes with potential risks and issues especially in terms of security. As the first phase discuss potential security risks for AMI. This phase, will discuss best practices to mitigate those security risks and benefiting the AMI Utilities.

3.4.3 Basic AMI Security Considerations[112]

Baseline security requirements can be classified by high-level functionality. These include confidentiality and privacy, integrity, availability, authentication and non-repudiation /accounting. The foundation of much of this functionality is based on cryptographic services including cryptographic key management and cryptographic operations for a number of purposes, including to:

- Cryptographically authenticate metering assets to the network to ensure that only known and approved devices participate in the network
- Authenticate and integrity check system commands, at the meter, to ensure they are authorized and haven't been tampered
- Guard against replay attacks to prevent denial of service attacks or load shedding and ensure availability of system resources
- Encrypt meter data to protect consumer privacy
- Provide a means of non-repudiation for consumer demand response programs
- Provide integrity protection and origin authentication of meter data.
- Authenticate and integrity check meter firmware and configuration images when updates are provisioned.
- Adopt an open reference standard for security of advanced meters.
- Enforce full implementation of the security standard by advanced meter vendors.
- Authenticate all commands from the head-end to the customer endpoint.
- Authenticate all reporting from the customer endpoint to the head-end.
- Protect head-end systems as if they were critical cyber assets in the sense of NERC CIP-002.
- Implement host-based intrusion detection with software integrity checking of the headend systems.
- Perform frequent, irregularly scheduled audits of head-end outputs to ensure they reflect inputs.
- Use strong user authentication on all head-end systems and log all user actions.
- Implement network separation, strong firewalls, and limited router access control lists in the AMI network.

[112] http://www.oe.energy.gov/DocumentsandMedia/20-AMI_Security_Considerations.pdf

- Implement strong separation between the AMI network and the electronic security perimeters of other systems such as EMS.
- Implement safety logic to prevent rapid changes in pricing information sent from the head-end to the customer endpoint.

Beyond baseline cryptographic services, systems and processes are also needed to manage assets in a secure fashion. For instance, system keys must be protected from disclosure through physical and policy-based mechanisms. Role based access controls should authenticate utility operations personnel authorized to manage the system and provide a secure audit trail when system management or maintenance tasks, such as updating of keys is performed.

3.4.3.1 Code Signing and Firmware Authentication

Code signing[113]:

It is a mechanism whereby publishers of software and content can use a certificate-based digital signature to verify their identities to users of the code, thus allowing users to decide whether or not to install it based on whether they trust the publisher. Code signing is based on the use of a digital signature, which is in turn is based on a digital certificate issued by a trusted third party (a certification authority) that has verified the identity of the software or content publisher. When a developer enrolls for a digital ID, he is required to submit documentation of proof of identity. A public/private key pair is generated when the certificate is requested. The private key stays on the requester's computer and is never sent to the CA. It should not be shared with anyone. The public key is submitted to the CA with the certificate request.

After the certificate is issued, the developer uses the private key associated with that public key to sign his code. When users download the signed code, they get a copy of the certificate verifying the identity of the author/publisher. The Web browser verifies the digital signature, and the user knows that the code did indeed come from that particular developer.

Here is exactly what happens when a developer signs the code:

1. The code is put through a one-way hash function. This creates a "digest" of fixed length.
2. The developer's private key is used to encrypt this digest.
3. The digest is combined with the certificate and hash algorithm to create a signature block.
4. The signature block is inserted into the portable executable file.

What happens at the other end (on the computer that downloads the signed code)? Here's the process:

1. The certificate is examined and the developer's public key is obtained from the CA.

---

[113] Deb Shinder, "Code Signing: Is it a Security Feature?" http://www.windowsecurity.com/articles/Code-Signing.html Window Security, June 2005.

2. The digest is then decrypted with the public key.
3. The same hash algorithm that was used to create the digest is run on the code again, to create a second digest.
4. The second digest is compared to the original.

If the two digests match, you know that the public key is the one that matches the private key used to sign the code, and you know that the code hasn't been changed since it was signed.

A key step in building a strong security foundation is to establish a root of trust for every device. This enables each device to validate its operating environment, including any modifiable software or configuration files. It is when firmware is being reprogrammed that devices can be most vulnerable. To ensure image code integrity and authenticity, the core boot loader should be stored in protected (read only) memory. Signatures should authenticate firmware and sensitive configuration data. In order for those signatures to be legitimate, OEM authentication keys should also be protected from unauthorized modification – preferably stored in one-time-programmable (OTP) memory. Configuration data should be bound to the device identity, such as a unique MAC address.

3.4.4 Best Practices for the Security Issues

3.4.4.1 For Customer Threat

The AMI industry and operators could mount an effective defense against abusive customers by using a data transmission standard for AMI data and investigating abnormal usage patterns. In addition to that, customer endpoint as access to exploit the AMI network can be prevented by implementing network control defenses such as router access lists and firewalls within the AMI network. When doing so, the utility will need to consider each of the points at which the communication changes networks to ensure that attackers can't bypass defenses by jumping into the middle of the network. Some AMI architectures call for several transitions from one communication network to another, including wireless communication at points upstream from the customer endpoint.

3.4.4.2 The terrorist and nation-state threats

They can be mitigated by all of the above because they make the target less attractive. Additional effective approaches to protecting against this threat are router access lists, firewalls, protected communication between the AMI network and other networks, strong communication authentication, and detection and halting of rapid market fluctuations.

To organize the security issues in different areas of AMI, below is the described table for best practices for each of the areas.

3.4.5 Best Practices for different areas of Security[114]

Refer to Appendix B for some of the best practices with detail description, which we have used as acronyms in the threat and best practices tables (Table 3-19 through Table 3-30).

3.4.5.1 Admin Threats

Administrative threats are those threats that are caused by malicious or negligent administrators. These threats are listed below in Table 3-19.

Table 3-19: Admin Threats: Best Practices

Threat Name	Description	Best Practices
1	An entity gives access to information assets to inappropriate users	Admin_Roles_Access Confidentiality Rollback Session_Protection Security_Mgt Security_Roles Attr_based_Policy Secure_Configuration User_Auth_Management Enrollment_Process I&A
2	An AMI entity with proper access gives access to resource assets to inappropriate users	
3	An AMI entity with proper access gives access to service assets to inappropriate users	
4	An AMI entity with proper access enrolls a user with inappropriate levels of access control. .	
5	An entity uses the Lockout service asset in an unauthorized manner to lock out a user.	
6	An entity uses the Lockout service asset in an unauthorized manner to unlock a locked out a user.	
7	An AMI entity with access creates a large policy causing an exhaustion of storage space.	Admin_Roles_Access Confidentiality

[114] http://osgug.ucaiug.org/utilisec/amisec/Shared%20Documents/Forms/AllItems.aspx?RootFolder=%2futilisec%2famisec%2fShared%20Documents%2f0.%20AMI%20Risk%20Assessment&FolderCTID=&View={7B63C81F-617F-4FC1-AFCB-8404B6B6B0A7}

Threat Name	Description	Best Practices
8	An AMI entity without proper access exploits policy flaws to gain improper (unintended) access to assets.	Rollback Session_Protection Security_Mgt Security_Roles Attr_based_Policy Secure_Configuration User_Auth_Management Enrollment_Process I&A
9	An AMI entity with access enters/modifies AMI policy incorrectly, due to a lack of understanding of the policy system.	
10	An AMI entity with access enters/modifies AMI policy incorrectly, due to a lack of understanding of the current policy.	
11	An AMI entity with access enters/modifies AMI policy maliciously to cause information disclosure or loss.	
12	An AMI entity with access enters inconsistent AMI policy.	
13	An AMI entity with access imports a malicious AMI organizational policy.	
14	Required organizational policies are inconsistent resulting in denial of service.	

Audit Threats

Audit threats are those threats that involve the AMI audit logs.

Table 3-20: Audit Threats: Best Practices

Threat Name	Description	Best Practices
1	An entity creates a large number of auditable events in order to cause the AMI audit logs to run out of resource space.	Audit_Log_Maintenance Import_Export_Control Maintain_Online
2	An AMI entity with proper access to the audit logs fails to clear enough space for the logs, causing the AMI audit logs to run out of resource space.	
3	An entity causes the AMI auditing function to fail, allowing an entity to perform non-recorded auditable actions.	

Threat Name	Description	Best Practices
4	An entity reads AMI audit logs when it does not have authorization to read any audit logs.	Audit Confidentiality Import_Export_Control I&A Maintain_Online Attr_based_Policy Admin_Guidance
5	An entity reads AMI audit logs with a security attribute it does not possess.	
6	An entity modifies AMI audit logs to hide other actions.	
7	An entity deletes AMI audit logs it does not have authorization to delete.	
8	An AMI entity with proper access misinterprets audit data, and thus cannot detect inappropriate actions of other principals.	
9	An AMI entity with proper access cannot find the desired audit data within the AMI audit logs, and thus cannot detect inappropriate actions of other principals.	Audit Import_Export_Control Maintain_Online Admin_Guidance Audit Import_Export_Control Maintain_Online Admin_Guidance
10	An AMI entity with proper access is not provided enough information by the AMI audit logs to detect inappropriate actions of other principals.	
11	An AMI entity with proper access is not provided enough information by the AMI audit logs to identify principals who take inappropriate actions.	

Download Threats

Download threats are those threats that directly involve the download source interface (patch software, etc).

Table 3-21: Eavesdropping Threats: Best Practices

Threat Name	Description	Best Practices
1	An entity eavesdrops on the Backhaul network in an attempt to read an information asset (e.g., in order to receive covert channel communications or perform traffic analysis).	O.Confidentiality O.Crypto_Comm_Channel O.Import_Export_Control
2	An AMI entity eavesdrops on the AMI Virtual Network in an attempt to read an information asset (e.g., in order to receive covert channel communications or perform traffic analysis).	
3	An entity eavesdrops on the Policy Authority Interface in an attempt to read a policy, policy mechanism, or traffic flow information asset.	
4	An entity eavesdrops on the AMI Systems Interface in an attempt to read information content, information attributes, policy, policy mechanism, or traffic flow information assets.	
5	An entity eavesdrops on the non-AMI Systems Interface in an attempt to read information content, information attributes, or traffic flow information assets.	
6	An entity eavesdrops on the Key Management Systems Interface in an attempt to read policy, policy mechanisms, or traffic flow information assets.	
7	An entity eavesdrops on the Users Interface (e.g. via a camera or a tap in the monitor cable) in an attempt to read policy, information content, or information attributes information assets.	Confidentiality Import_Export_Control Session_Protection
8	A valid AMI user leaves the workstation unattended, does not logout, and leaves the AMI Token in the workstation. An entity sits at the unattended workstation and improperly accesses information assets.	Confidentiality Session_Protection

Threat Name	Description	Best Practices
9	An entity eavesdrops on the Users Interface because an authorized user viewed information assets in an unauthorized area.	Security_Mgt Comp_Attributes Physical_Security

Identification & Authentication Threats

I&A threats are those threats that involve the user identification and authentication process.

Table 3-22: Identification and Authentication Threats: Best Practices

Threat Name	Description	Best Practices
1	An entity discovers user authentication information from an AMI component resource asset.	Confidentiality I&A
2	An entity discovers user authentication information by external methods (i.e. human intelligence).	
3	An AMI entity attempts to crack I&A mechanisms through brute force methods (e.g., a password cracker).	
4	An entity is able to guess a passphrase because the passphrase was too simple (e.g., too short, it is “password”, etc.)	

Table 3-23: Downloading Threats: Best Practices

Threat Name	Description	Best Practices
1	An AMI entity with proper access to the Download service asset loads software/configuration into an AMI component resource asset out of sequence.	Import_Export_Control Integrity_Checks SW_Download

2	An AMI entity with access to the Download Software service asset loads software/configuration into the wrong AMI component resource asset.	Confidentiality Import_Export_Control Integrity_Checks SW_Download Comp_Attributes

3.4.5.2 Eavesdropping Threats

Eavesdropping is unauthorized real-time interception of a private communication.

Several Solutions:

- Provide secure session establishment between the system and remote systems using NSA approved confidentiality, integrity, authentication and non-repudiation of network transmissions.
- Restrict user access to cryptographic IT assets in accordance with a specified user access control policy.
- Provide complete separation between plaintext and encrypted data and between data and keys.
- Provide security services and labels on import/export data that is consistent with policy (i.e. user, data source, data content, and intended audience).
- Provide protection of a user or admin session to prevent an unauthorized user from using an unattended computer where a valid user has an active session.

Table 3-24: Eavesdropping Threats: Best Practices

Threat Name	Description	Best Practices
1	An entity eavesdrops on the Backhaul network in an attempt to read an information asset (e.g., in order to receive covert channel communications or perform traffic analysis).	O.Confidentiality O.Crypto_Comm_Channel
2	An AMI entity eavesdrops on the AMI Virtual Network in an attempt to read an information asset (e.g., in order to receive covert channel communications or perform traffic analysis).	O.Import_Export_Control
3	An entity eavesdrops on the Policy Authority Interface in an attempt to read a policy, policy mechanism, or traffic flow information asset.	

Threat Name	Description	Best Practices
4	An entity eavesdrops on the AMI Systems Interface in an attempt to read information content, information attributes, policy, policy mechanism, or traffic flow information assets.	
5	An entity eavesdrops on the non-AMI Systems Interface in an attempt to read information content, information attributes, or traffic flow information assets.	
6	An entity eavesdrops on the Key Management Systems Interface in an attempt to read policy, policy mechanisms, or traffic flow information assets.	
7	An entity eavesdrops on the Users Interface (e.g. via a camera or a tap in the monitor cable) in an attempt to read policy, information content, or information attributes information assets.	Confidentiality Import_Export_Control Session_Protection
8	A valid AMI user leaves the workstation unattended, does not logout, and leaves the AMI Token in the workstation. An entity sits at the unattended workstation and improperly accesses information assets.	Confidentiality Session_Protection
9	An entity eavesdrops on the Users Interface because an authorized user viewed information assets in an unauthorized area.	Security_Mgt Comp_Attributes Physical_Security

Identification & Authentication Threats

I&A threats are those threats that involve the user identification and authentication process.

Table 3-25: Identification and Authentication Threats: Best Practices

Threat Name	Description	Best Practices
1	An entity discovers user authentication information from an AMI component resource asset.	Confidentiality I&A

Threat Name	Description	Best Practices
2	An entity discovers user authentication information by external methods (i.e. human intelligence).	
3	An AMI entity attempts to crack I&A mechanisms through brute force methods (e.g., a password cracker).	
4	An entity is able to guess a passphrase because the passphrase was too simple (e.g., too short, it is “password”, etc.)	

3.4.5.3 Insider Threats

Insider threats are those threats that directly involve authorized users of the system operating maliciously or negligently. Abnormal insider activity should be detected with high probability, since individual insider threats are negated by discovery. Publicizing the improved detection capability also reduces risk by deterring insider activity. Background checks and audits, authentication, intrusion detection, and software integrity checking are all relevant in this role. Further, it is sensitive to being caught (low goal intensity) so the best defenses against insiders are those that increase the deterrent effect by increased chance of detecting the activity. First, all communication from the head-end to the customer endpoint should be treated as control traffic. As such, authentication of commands should be put in place. Good authentication will prevent man-in-the-middle and spoofing attacks by insiders with access to the AMI communication network. While the head-end systems are clearly not critical cyber assets in the sense of NERC CIP-002 (Cyber security standard by NERC)[115], the utility may want to treat them as such, and implement personnel and system security management. Measures such as background checks and auditing will deter insiders who attack through physical access to AMI or related systems. Host-based intrusion detection with software integrity checking of the head-end systems will detect changes to the systems by insiders. Utilities should conduct frequent, irregular audits of head-end output compared against input to ensure that they match. All user commands and actions in the head-end systems should be accountable, which will require logging and strong user authentication.

[115] http://www.nerc.com/files/CIP-002-1.pdf

Table 3-26: Insider Threats: Best Practices

Threat Name	Description	Best Practices
1	An AMI entity with access creates, enters, edits, or imports content and labels it with incorrect security attributes resulting in unauthorized disclosure.	Confidentiality Import_Export_Control
2	An AMI entity with access to an information asset attempts to exfiltrate that information asset to a potential covert channel.	Confidentiality Import_Export_Control
3	An AMI entity with access to an information asset prints that asset and discloses it to an inappropriate individual.	

3.4.5.4 Key Management Threats

Key Management threats are those threats that involve the Key Management Systems with which AMI interfaces.

Table 3-27: Key Management Threats: Best Practices

Threat Name	Description	Best Practices
1	An AMI entity with proper access to the Deliver Keys service asset downloads duplicate keys with different attributes. This can lead to unauthorized access to assets.	Confidentiality Admin_Guidance Crypto_Key_Man
2	An AMI entity with proper access to the Deliver Keys service asset downloads weak keys that can be broken. This can lead to unauthorized access to assets.	
3	An AMI entity with proper access to the Deliver Keys service asset downloads keys with inappropriate attributes. This can lead to unauthorized access to assets.	

Threat Name	Description	Best Practices
4	An AMI entity with access to the Membership Management service asset fails to report an individual whose keys should be revoked.	Admin_Roles_Access Confidentiality Admin_Guidance User_Auth_Management
5	Key Management services evolve in ways that are not backwardly compatible with AMI (may be included in KMS).	Crypto_Key_Man

3.4.5.5 Malicious Code

Malicious code threats are those threats that involve malicious code execution or implantation.

Table 3-28: Malicious Code Threats: Best Practices

Threat Name	Description	Best Practices
1	An entity implants malicious code in an application in order to modify the operating system, other applications, or data leading to disclosure of information assets, modification of information assets, denial of service, repudiation.	Confidentiality Integrity_Checks Isolate_Executables Malicious_Code Attr_based_Policy
2	An entity implants malicious code in an application in order to modify the operating system, other applications, or data leading to exfiltration of information assets to potential covert channels.	
3	An entity implants malicious code in an application in order to attack external entities through an AMI interface.	
4	An entity implants malicious code in an information asset in order to gain access to an asset it is not authorized to access.	
5	An entity implants malicious code in an information asset in order to exfiltrate information assets to a potential covert channel.	
6	An entity implants malicious code in an AMI component information asset in order to modify information assets.	

Threat Name	Description	Best Practices
7	An entity causes a user to execute malicious code in an AMI component information asset in order to modify information assets.	Integrity_Checks Isolate_Executables Malicious_Code
8	An entity causes a user to execute malicious code in an information asset in order to gain access to an asset.	Confidentiality Integrity_Checks Isolate_Executables Malicious_Code
9	An entity causes a user to execute malicious code in an information asset in order to exfiltrate information assets to a potential covert channel.	
10	An entity implants malicious code in an AMI component resource asset in order to gain access to an asset.	Confidentiality Integrity_Checks Isolate_Executables Malicious_Code Attr_based_Policy
11	An entity implants malicious code in an AMI component resource asset in order to exfiltrate information assets to a potential covert channel.	
12	An entity implants malicious code in an AMI component resource asset in order to modify information assets.	
13	An entity causes a user to execute malicious code in an AMI component resource asset in order to gain access to an asset it is not authorized to access.	Integrity_Checks Isolate_Executables Malicious_Code
14	An entity causes a user to execute malicious code in an AMI component resource asset in order to exfiltrate information assets to a potential covert channel.	

3.4.5.6 Operational Denial of Service (DOS) attack

Operational denial of service threats are those threats that affect availability of the system and may be caused by operational users of the system.

Table 3-29: Operational Denial of Service Attacks: Best Practices

Threat Name	Description	Best Practices
1	An entity enters access control attributes related to specific content resulting in denying access to consumers who should be authorized for that information object.	Import_Export_Control I&A Integrity_Checks Integ_Data NonRepudiation Obj_Attr Session_Protection User_Attributes Attr_based_Policy User_Guidance
2	An entity enters improper value in the priority attribute related to specific content resulting in reduced distribution efficiency for that information object.	
3	An entity creates excessive volume of information objects resulting in resource exhaustion (e.g., storage space) resulting in a denial of service.	I&A NonRepudiation Resource_Quotas Session_Protection User_Attributes Attr_based_Policy

Threat Name	Description	Best Practices
4	An entity removes or changes endorsements on an information object in an unauthorized manner with the intent to stop the publication of the information object.	Import_Export_Control I&A Integrity_Checks Obj_Attr Session_Protection User_Attributes Attr_based_Policy
5	An entity enters (regrades to) incorrect values in the access control attributes that overly restrict access to the information content resulting in denial of service. Incorrect values could be as a result of: • Negligence • Hidden or malicious content • Content different than what was displayed	Import_Export_Control I&A Integrity_Checks Obj_Attr Session_Protection User_Attributes User_Guidance Attr_based_Policy Resource_Quotas
6	An entity publishes the information object to an excessive volume of ownership types resulting in resource exhaustion (e.g., storage space).	
7	An entity deletes an object it is not authorized to delete resulting in denial of service.	I&A

Threat Name	Description	Best Practices
8	An AMI entity deletes an object it is authorized to delete resulting in denial of service.	Integrity_Checks Obj_Attr Priority_Of_Service Session_Protection User_Attributes Attr_based_Policy NonRepudiation

3.4.5.7 Operational Integrity Threats

Operational integrity threats are those threats that affect integrity of the system or information in the system and may be caused by operational users of the system.

Table 3-30: Operational Integrity Threats: Best Practices

Threat Name	Description	Best Practices
1	An entity modifies an information asset it is not authorized to modify.	I&A Integrity_Checks Integ_Data Obj_Attr Session_Protection User_Attributes Attr_based_Policy
2	An entity modifies information content it is not authorized to modify	
3	An entity modifies access control attributes when it does not have regrade function access	
4	An entity modifies information attributes it is not authorized to modify	
5	An entity modifies policy it is not authorized to modify	

Threat Name	Description	Best Practices
6	An AMI entity with access in a remote information system attempts to modify AMI information objects in an unauthorized manner.	I&A Integrity_Checks Integ_Data Obj_Attr Session_Protection
7	An entity modifies an AMI component software or operating system resource asset in an unauthorized manner.	I&A Integrity_Checks Integ_Data Obj_Attr Session_Protection User_Attributes Attr_based_Policy

3.4.5.8 Operational Non-Repudiation Threats

Operational non-repudiation threats are those threats that affect the ability to perform non-repudiation of information in the system and may be caused by operational users of the system.

Table 3-31: Operational Non- Repudiation Threats: Best Practices

Threat Name	Description	Best Practices
1	An entity enters, edits unauthorized values in the information attributes resulting in false attribution of the content creator.	Import_Export_Control I&A
2	An entity enters, edits unauthorized values in the information attributes resulting in false attribution of the information object copier. (X says Y did it)	NonRepudiation

Threat Name	Description	Best Practices
3	An entity improperly enters, edits unauthorized values in the information attributes resulting in false attribution of the content endorser. (X says Y signed it).	Session_Protection User_Attributes Attr_based_Policy

3.4.5.9 Social Engineering Threats

Social engineering threats are those threats that involve human-to-human breaches in security.

Table 3-32: Social Engineering Threats: Best Practices

Threat Name	Description	Best Practices
1	An entity co-opts an AMI user to grant the entity system access.	Confidentiality I&A Physical_Security
2	An entity persuades a user of a non-AMI system with some level of access to AMI to divulge his AMI credentials.	Confidentiality
3	An entity persuades a user of a different AMI system with some level of access to the AMI to divulge his AMI credentials.	Confidentiality
4	An entity persuades an administrator of a non-AMI system to reveal information about system operational procedures, auditing or known flaws so as to enable the entity to access AMI.	Confidentiality Secure_Configuration Evaluated_System
5	An AMI entity co-opts an AMI user to grant the entity authorization to an asset.	Confidentiality I&A Physical_Security

Threat Name	Description	Best Practices
6	An entity co-opts an AMI user to access information assets. The attacking entity may then access the information via the co-opted user (e.g., read over the shoulder of user, have user verbally tell content).	Confidentiality User_Attributes User_Auth_Management Physical_Security
7	An entity co-opts an AMI user to exfiltrate information assets to a potential covert channel.	Confidentiality User_Auth_Management Secure_Configuration User_Auth_Management
8	An entity co-opts an AMI user to modify information assets.	
9	An entity attempts to guess a user passphrase based upon knowledge of the user.	Confidentiality I&A User_Auth_Management

3.4.5.10 Flawed Implementation Threats

Flawed implementation threats are those threats that arise due to an incorrect or insecure implementation of AMI. Specific threats are listed below.

Table 3-33: Flawed Implementation Threats: Best Practices

Threat Name	Description	Best Practices
1	An entity exploits flaws in the AMI component [software, hardware] resource assets to gain improper access to assets.	Confidentiality SW_Download Malicious_Code Evaluated_System
2	An entity exploits flaws in the AMI component [software, hardware] resource assets to perform a denial of service attack.	
3	An entity exploits flaws in the AMI component [software, hardware] resource assets to exfiltrate an information asset.	

3.5 Countermeasures for SCADA Vulnerabilities:

SCADA system generally refers to monitoring and controlling of equipment that are responsible for delivering power in Smart Grid. Extended functionality of SCADA includes fault detection, equipment isolation and restoration, load and energy management, automated meter reading, and substation control. The SCADA systems used today by the utilities were developed and deployed many years ago. At that time there was no internet, public or private network. Hence, the only security threat was physical destruction of the systems. However, with the introduction of equipment automation and deregulation, SCADA systems needed to have some kind of interconnected network. The need for the remote connections to these control devices exposed the network to a completely new set of vulnerabilities[116].

SCADA system works with the corporate environment though it was originally designed to operate as an individual unit. The core intention of the control system design is efficiency and security. Communication protocols like DNP3 which is used for SCADA are designed in order to facilitate communications between various types of data acquisition and control equipment. The protocol was not designed to be secure from hackers, malwares and other malevolent forces that could easily destroy the control systems and disable any critical infrastructure like SCADA. SCADA Network has lot of concern regarding the Security, Authenticity and Integrity in its design, deployment and operation[117].

These above mentioned design, communication and behavioral patterns are reasons for the security weakness of the SCADA system. These vulnerabilities in a SCADA like critical infrastructure make it very susceptive to cyber attacks. Following are the counter measures which need to be implemented in order to make the SCADA system more secure.

3.5.1 Countermeasures for Master Terminal Unit and Remote Terminal Unit Security Issues

SCADA system consists of Master Terminal Unit (MTU) and Remote Terminal Unit (RTU) as some of the major components. The other components include communication equipment and SCADA software[118].

MTU will be located at central control facility of the operator. It enables the two way connect and control SCADA's physical equipment. It generally converts the electrical signals coming from the equipment into some digital value like open/closed switch. By receiving, converting and sending these signals, RTU can measure and control the pressure, flow, voltage and current.

---

[116]Edward Chikuni, Department of Electrical Engineering Polytechnic University of Namibia, Namibia, Maxwell Dondo, Defence R&D Ottawa, 2007 " Investigating the Security of Electrical Power Systems SCADA". [Online]
Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4401531&tag=1

[117] Wikipedia: DNP3. http://en.wikipedia.org/wiki/DNP3

[118] Scada System Assessment. http://www.nbtinc.com/scada-system-assessment.html NBT.

The potential and present vulnerabilities in MTU and RTU are due to the publicly available information, vulnerabilities in policy and procedures and also due to vulnerabilities in platform configuration.

Often, too much information about a utility company corporate network is easily available through routine public queries. In addition, significant information on control systems is publicly available—including design and maintenance documents, technical standards for the interconnection of control systems and RTUs, and standards for communication among control devices. This information can be used to initiate a more focused attack against the network[119]. Inadequate security policy for the SCADA, Lack of security procedure documentations and guidelines and improper security architecture and design adds up to the policy and procedure vulnerabilities.

Earlier SCADA hardware, software, and network protocols were proprietary and not made publicly accessible, making it more difficult for the hackers to attack the system as they did not have knowledge about the system. However with growing competition and drive to perform better and reduce cost has led organizations to make a transition from proprietary systems to standardized technologies such as Microsoft's windows, UNIX operating systems and common networking protocols used by the internet. As a result, the SCADA's platform got exposed to various vulnerabilities related to Operating Systems, Password and Access Control.

The security issues in the Master Terminal Unit (MTU) and Remote Terminal Unit (RTU) lie mostly within the platform and policy. The best practices for policy vulnerabilities are already explained in the introduction chapter. The following points further highlight the various ways to overcome these security issues.

3.5.1.1 Counter Measures for Policy and Procedure Vulnerabilities

Some of the potential vulnerabilities in the SCADA system as discussed by NIST (National Institute of Standards and Technology) in one of its papers presented on "Guide to Industrial Control Systems Securities" are[120]:

- Inadequate security policy for the SCADA
- No specific or documented security procedures were developed from the security policy for the SCADA
- Absent or deficient SCADA equipment implementation guidelines
- Lack of administrative mechanisms for security enforcement
- No formal SCADA security training and awareness program

---

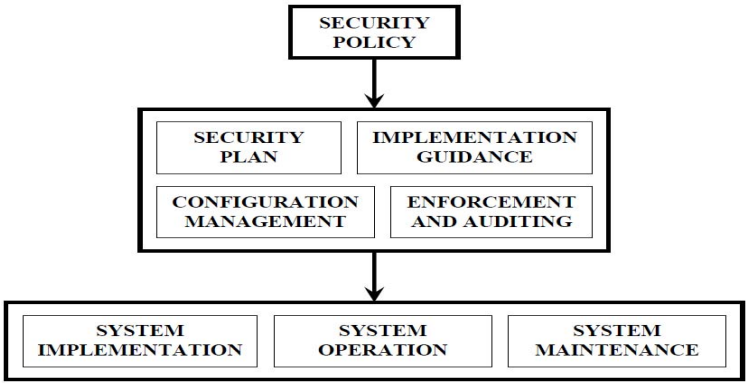
[119] Amanullah, International Islamic University Malaysia, A. Kalam, Victoria University of Technology, member, IEEE, and A. Zayegh, Victoria University of Technology, Australia. Member, IEEE 2005, "Network Security Vulnerabilities in SCADA and EMS". [Online] Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1546981&tag=1

[120] Keith Stouffer, Joe Falco, Karen Scarfone, NIST Sep 2008, "Guide to Industrial Control Systems (ICS) Security" [Online] Available: http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf

- Inadequate security architecture and design
- Few or no security audits on the SCADA
- No SCADA specific continuity of operations or disaster recovery plan (DRP) and
- Lack of SCADA specific configuration change management

The Information Security Policy in the introduction chapter explains best practices to overcome the policy related vulnerabilities. Figure 3-19 is used to implement the general security policies and procedure. The structure encompasses all the security features that need to be covered in a security policy which can also be applied to SCADA[121].

Figure 3-19: Basic Functions of Security Policy



3.5.1.2 Regular Vulnerability Assessments

All the SCADA equipment has to be regularly assessed to check and see if there is an abnormal operations taking place. These assessments must be done in a regular basis and should be recurring. Along with the operational units, the other components of SCADA like the corporate network, data base servers, local desktop computers used for customer management should be assessed so that any unseen security gaps in this system can be overcome and increase protection[122].

3.5.1.3 Expert Information Security Architecture Design

There are best practices that can be used to overcome most of the security issues in the network. Also a number of new technologies have been developed to combat vulnerabilities such as

---

[121]Jason Stamp, John Dillinger, and William Young, Networked Systems Survivability and Assurance Department, Jennifer DePoy, Information Operations Red Team & Assessments Department, Sandia National Laboratories Albuquerque, NM 87185-0785, 22 May 2003, "Common Vulnerabilities in Critical Infrastructure Control Systems". [Online] Available: http://www.oe.netl.doe.gov/docs/prepare/vulnerabilities.pdf

[122] Riptech, January 2001, "Understanding SCADA System Security Vulnerabilities", [Online] Available: http://www.iwar.org.uk/cip/resources/utilities/SCADAWhitepaperfinal1.pdf

malware attacks, unauthorized access to systems which are briefly explained in Description section of the Introduction chapter.

3.5.1.4 Implementing Security Features Provided By Device and System Vendors

Older SCADA networks did not have many security features to protect the system. The utility companies which own the SCADA networks must ask the vendor to provide security patches to the existing system and also produce newer system with enhanced security features. Also factory default security features should not be used because their intent is to provide excellent usability and provide the minimum amount of security. When the default settings are being changed and are not set to its maximum security limits, a thorough risk assessment must be done before those levels are fixed.

3.5.1.5 Establishing Strong Controls over Any Medium That Is Used As Backdoor Into SCADA Network

Strong authentication must be implemented to ensure secure communications where backdoors vendor connections exist in SCADA system. Modems, wireless and wired networks used for communications and maintenance represent a significant vulnerability to the SCADA network and remote sites. Sending false packets from the enterprise network can attack SCADA system if the SCADA system does not authenticate the packet. It needs to check if the packet is from a authenticate source and only then process the packet. Authentication methods such as challenge response, hashing algorithms and digital signatures can be used.

3.5.1.6 Implementing Internal and External Intrusion Detection Systems and Establishing 24-hour-a-day Incident Monitoring

When abnormal sequence of events takes place on the SCADA network there must be some way to inform the network administrators about this activity. This can be done by using intrusion detection mechanisms where 24 hours tracing of events on the network is recorded. When a security incident takes place either from internal or external sources then there should be techniques and procedures to immediately overcome them based on the level of damage it can cause. To complement network monitoring, enable logging on all systems and audit system logs daily to detect suspicious activity as soon as possible.

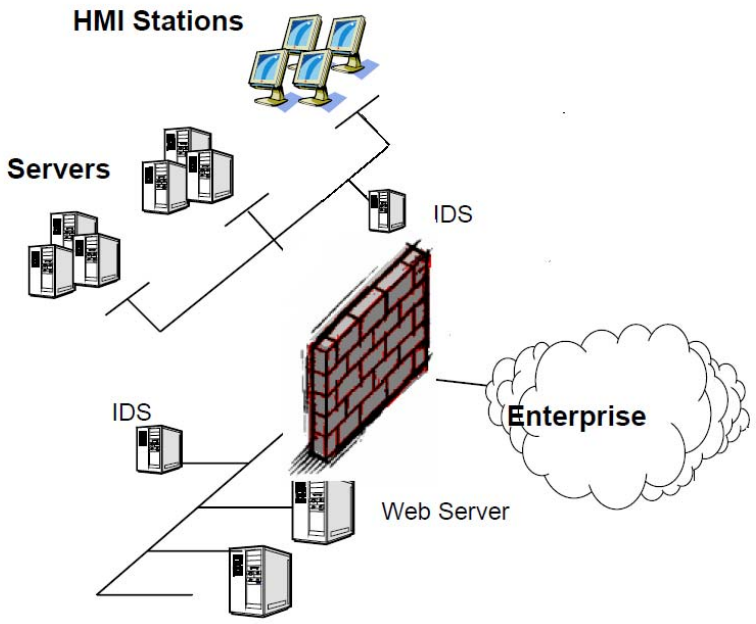
3.5.1.7 Conducting Physical Security Surveys and Assessing All Remote Sites Connected To SCADA Network

Automated systems in the SCADA network are most susceptible to attacks since they are unmanned and unguarded. An inventory of all access points and carrying out physical security checks regularly will help to keep a check on any new security issues. Identify and assess any source of information including remote telephone/computer network/ fiber optic cables that could be tapped; radio and microwave links that are exploitable; computer terminals that could be accessed; and wireless local area network access points. Eliminate any points of failure. Prevent unauthorized access to the websites within the enterprise intranet since they provide access to the SCADA system.

3.5.1.8 Utilizing Firewalls and Intrusion Detection System

Threats to SCADA network can come from malicious attackers via the internet and hence it is important to monitor the traffic that flows into it. It is important that firewalls and other Intrusion Detection Systems (IDS) (Figure 3-20) be installed at the various ingress points (gateways) of the SCADA network to identify malicious traffic before it is allowed to enter[123] [124]. This will filter out some of the attacks but not all. Hence more rigorous scheme needs to be implemented to overcome the attacks that still manage to flow through. Viruses and worms could swamp the systems with huge volumes of attack traffic. Just having only firewalls and IDS at entry points may not suffice. This leads to the concept of the electronic perimeter.

Figure 3-20: Firewall and Intrusion Detection System Implementation between Enterprise and SCADA Control System



3.5.1.9 Electronic Perimeter

Traffic flowing from outside sources reaches the gateway where a firewall restricts malicious packets and allows the rest to flow through. The traffic that flows through might still have some malicious packets which could harm the system. Beyond this gateway there is not much

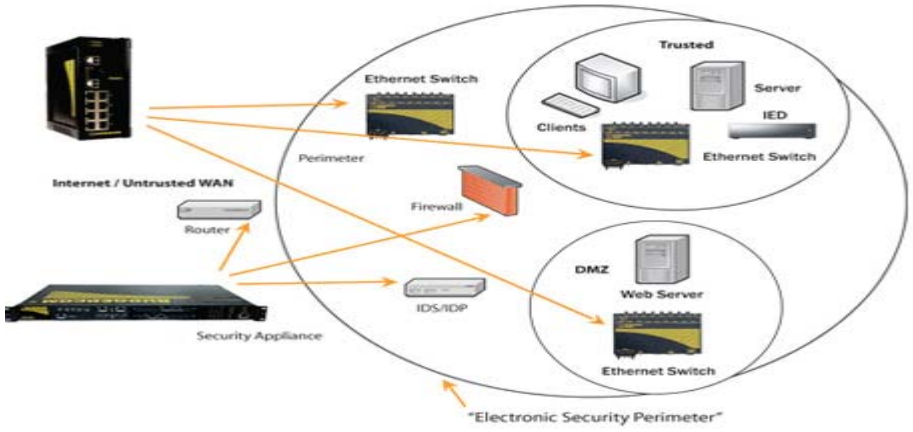
---

[123] Chee-Wooi Ten, Student Member, IEEE, Iowa State University, Manimaran Govindarasu, Member, IEEE, Iowa State University, and Chen-Ching Liu, Fellow, IEEE, Iowa State University 2007, "Cyber security for Electric Power Control and Automation Systems". [Online]
Available: http://powercyber.ece.iastate.edu/publications/SMC-conf.pdf

[124] Dale Peterson, Director, Network Security Practice Digital Bond, Inc, "Intrusion Detection and Cyber Security Monitoring of SCADA and DCS Networks". [Online]
Available: http://www.isa.org/filestore/Division_TechPapers/GlassCeramics/TP04AUTOW046.pdf

filtering that takes place and hence it is important to define and electronic perimeter (Figure 3-21) broader so that it filtering takes place once before data reaches the gateway[125]. This perimeter can be formed by multiple intrusion detection systems installed on a wider area. Huge volumes of traffic can be handled by an extended perimeter as it would be possible to stop the attacks further away from the SCADA network. This provides a number of advantages of providing an overlay network in a more distributed and collaborative fashion. It also provides a barrier that always only legal traffic through.

Figure 3-21: Electronic Perimeter Implementation in SCADA System126



3.5.1.10 Domain-Specific IDS

The above-mentioned methods i.e. intrusion detection systems installation and electronic perimeter make a baseline protection to provide normal system behavior. In addition, a perspective on an intrusion can be developed by analyzing emerging characteristics. SCADA data can be analyzed in order to look for such patterns. To identify these patterns it is important to have some basic knowledge which is domain specific and also associated with communication devices to construct an IDS attacks signature database. It would require intense analysis of the interconnected grid in order to identify the attack patterns and study them and then generate signatures. However, once this is achieved, the observed behavior needs to be correlated to detect potential intrusions and filter the attack traffic[127]. Hence IDS with these

---

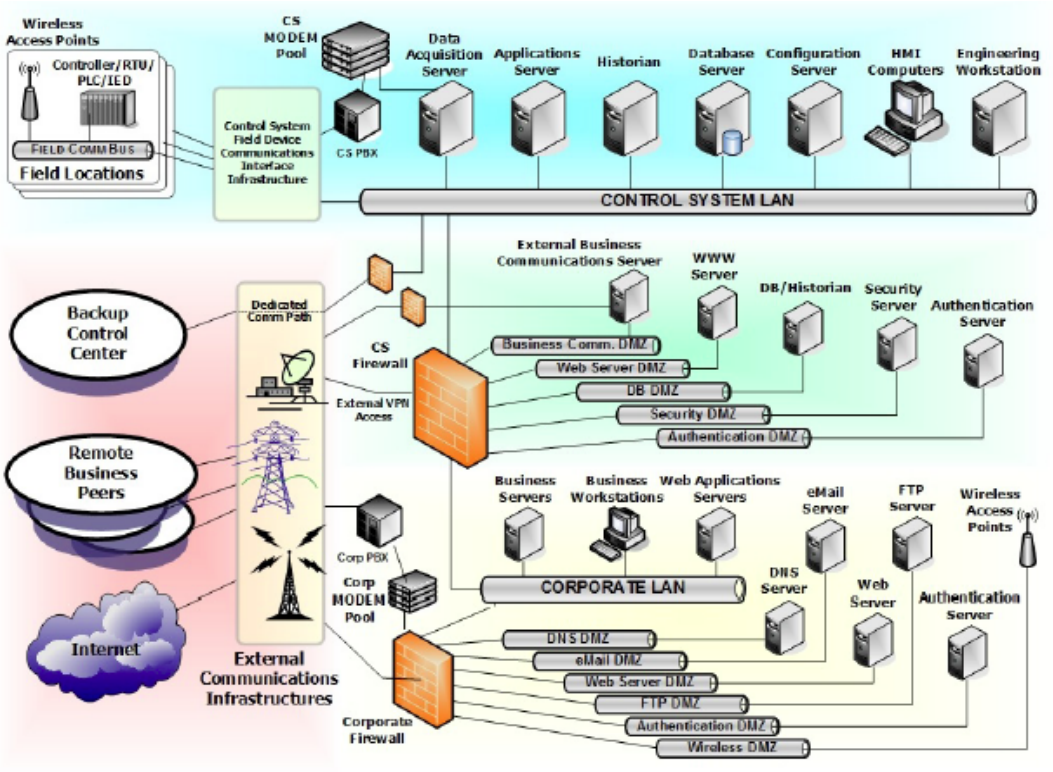
[125] Chee-Wooi Ten, Student Member, IEEE, Iowa State University, Manimaran Govindarasu, Member, IEEE, Iowa State University, and Chen-Ching Liu, Fellow, IEEE, Iowa State University 2007, "Cyber security for Electric Power Control and Automation Systems". [Online]
Available: http://powercyber.ece.iastate.edu/publications/SMC-conf.pdf
[126] Ruggedcom, "Typical Cyber Security Network Architecture" [Online]
Available: http://www.ruggedcom.com/applications/cyber-security/
[127] Chee-Wooi Ten, Student Member, IEEE, Iowa State University, Manimaran Govindarasu, Member, IEEE, Iowa State University, and Chen-Ching Liu, Fellow, IEEE, Iowa State University 2007, "Cyber security for Electric Power Control and Automation Systems". [Online]

signatures and the secure electronic perimeter can be made to work in a synchronized manner to combat the security issues posed by malware.

3.5.1.11 Creating Demilitarized Zones (DMZs)

Demilitarized Zones created using firewalls can protect the SCADA network. Multiple DMZs can be created to separate functionalities and access privileges such as peer to peer connections, the data historian, security servers, configurations servers etc. The figure 3-22 below shows the creation of DMZs.

Figure 3-22: Demilitarized Zones Architecture



All the connections can be routed through firewalls and administrators keep a diagram of the local area network and its connections to protected subnets, DMZs, the corporate network, and the outside. Multiple demilitarized zones help from attacks such as virtual LAN hopping, trust exploitation and bring in a better security posture[128].

3.5.1.12 Low Latency and High Integrity Security Solution Using Bump In the Wire Technology for Legacy SCADA Systems

The legacy SCADA systems, deployed without security in mind, are vulnerable to sniffing and tampering issues today. The risk is increasing because security through obscurity is failing to

---

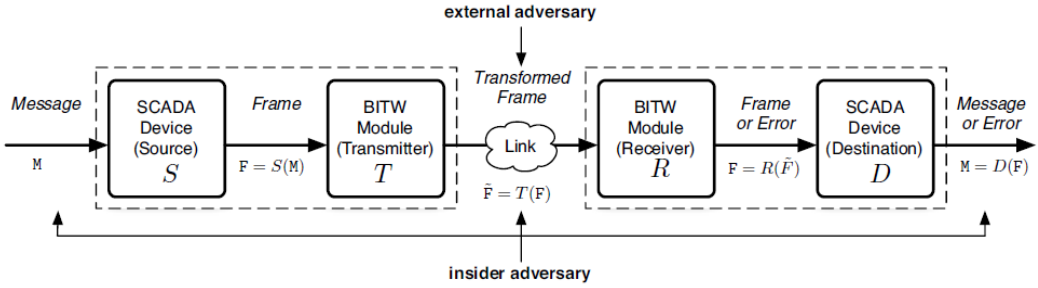
Available: http://powercyber.ece.iastate.edu/publications/SMC-conf.pdf

[128]Idaho National Laboratory, "Control Systems Cyber Security: Defense in Depth Strategies" [Online] Available: http://csrp.inl.gov/Documents/Defense%20in%20Depth%20Strategies.pdf

protect the system. Achieving security requires a solution, which can retrofit into the legacy SCADA system.

One such solution is "Yet Another Security Retrofit" (YASIR) which is a bump in the wire (BITW) solution for retrofitting security to time-critical communications in serial-based SCADA systems[129]. The goals are to provide high security, low latency, at comparable cost and using standard and patent free tools.

Figure 3-23: Model for Bump in the Wire Approach



In the figure above, the function of device denoted as S applied on message M which results in frame F. At the receiving end the function of device denoted as D is applied on the message received F'. BITW solution adds to more modules i.e. transmitter T and receiver R in order to provide data authenticity and discards messages from replay attacks.

In the design of transmitter and receiver in YASIR approach, the transmitter applies the encryption algorithm AES-CTR-128 on the frame F thereby providing confidentiality and integrity for the message. Then a time stamp and a unique sequence number are appended to the message for data authenticity and freshness. This solution also provides low latency by using the AES-CTR algorithm. The transmitter relies on the stream nature of the AES-CTR. As and when each byte of the frame F comes in, it will apply the encryption. There is an internal counter, which keeps a count of every 4 bytes in frame F. Once whole message is received it will use the HMAC on the cipher text and internal counter. An iterative HMAC function is used which reduces the storage requirements and has lesser latency[130].

---

[129] Tsang, P.P. and Smith, S.W., 2008, in IFIP International Federation for Information Processing, Volume 278; Proceedings of the IFIP TC 11 23rd International Information Security Conference; Sushil Jajodia, Pierangela Samarati, Stelvio Cimato; (Boston: Springer), pp. 445–459. [Online] Available: http://www.springer.com/computer/security+and+cryptology/book/978-0-387-09698-8

[130] Tsang, P.P. and Smith, S.W., 2008, in IFIP International Federation for Information Processing, Volume 278; Proceedings of the IFIP TC 11 23rd International Information Security Conference; Sushil Jajodia, Pierangela Samarati, Stelvio Cimato; (Boston: Springer), pp. 445–459. [Online] Available: http://www.springer.com/computer/security+and+cryptology/book/978-0-387-09698-8

3.5.2 Countermeasures for enhancing DNP3 Security

Distributed Network Protocol (DNP3.0) is used in the communication channel between the master and remote terminal unit. Vulnerabilities in the DNP3 protocol layers can be exploited to cause interruption, interception, modification and fabrication of communication between systems. The attacker can capture the message, analyze the traffic pattern, modify parameters such as length field, function code field, destination address, and sequence number field to cause denial of service. An attack on DNP3 takes place either by exploiting the specifications, vendor implementations or weaknesses in the infrastructure using DNP3. Vendor implementations are exploited by attacking the configurations errors in the system. Infrastructure attacks exploit the loop holes in the policies and platform.

3.5.2.1 Countermeasures

In order to combat the above attacks there must be solutions developed which make it more usable and hence provides reliability of data transmitted as well as protected data. In the following points, various solutions are proposed [131] [132] [133]and also how they used overcome the vulnerabilities in the system.

The Security Enhancement approaches are divided into three categories:

1. Solutions that wrap the DNP3 protocols without making changes to the protocols,
2. Solutions that alter the DNP3 protocols fundamentally, and
3. Enhancements to the DNP3 application.

The solutions that wrap the protocols include SSL/TLS and IPSec, which would provide a quick and low-cost security enhancement. The solutions that would require altering the DNP3 protocols tend to be more time-consuming to implement and expensive but provide better end-to-end security, (more application specific security).

3.5.2.2 Solutions That Wrap the DNP3 Protocols without Making Changes to Protocols

SSL/TLS Solution

Secure Sockets Layer (SSL)/Transport Layer Security (TLS) solution has been used over the internet to provide secure communication over TCP/IP. It provides mutual authentication

---

[131] Sandip Patel, Information Science & Systems at Morgan State University, Baltimore, Ganesh D. Bhatt, Department of Information Science & Systems at Morgan State University, James H. Graham, Electrical and Computer Engineering at the University of Louisville, July 2009, "Improving the Cyber Security of SCADA Communication Networks". [Online] Available: http://portal.acm.org/citation.cfm?id=1538788.1538820

[132] James H. Graham, Sandip C. Patel, Dept. of Computer Engineering and Computer Science, University of Louisville, September 2004, "Security Considerations in SCADA Communication Protocols". [Online] Available: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.84.1152

[133] Munir Majdalawieh1, Francesco Parisi-Presicce, Duminda Wijesekera, "DNPSec: Distributed Network Protocol Version 3 (DNP3) Security Framework". [Online] Available: http://www.acsac.org/2005/techblitz/majdalawieh.pdf

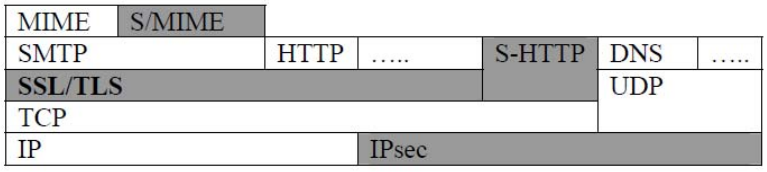
between the two end points and also preserves the integrity of the data by using digital signatures and privacy via encryption. They prevent man in middle attacks and replay attacks. Now by wrapping DNP3 with SSL/TLS have some advantages like it provides complete security at the protocol level implementation, it's a fast, effective and straight forward implementation, and also it is security standard for communication protocols.

IPSec (secure IP) Solution

Instead of providing security at the TCP level, security can be provided at the IP level using IPSec solution.

Since this is placed at a lower level in the stack, it not only protects the IP traffic but in turn protects the TCP traffic as well (See Figure 3-24). TCP solution of SSL/TLS could not protect from denial of service or connection reset attack since it was placed at a layer above TCP. But the IP Sec solution prevents entry of arbitrary packets and as well as connection reset because connection is done after it is inside the secured network layer. IPSec provides security for all the traffic since it is placed at the lowest level. This solution has some limitations like it is more sensitive to interference by intermediate devices in the communication path, it is less flexible in terms of security provided since it does not provide application specific security but just encrypts every packet and sends it irrespective of its application.

Figure 3-24: Protocol Stack



Gray-background protocols are secured alternatives

3.5.2.3 Enhancements to DNP3 Applications

The SSL/TLS solution and IPSec solution lack in providing end to end security. Therefore cryptographic techniques can be used in order to provide this level of security.

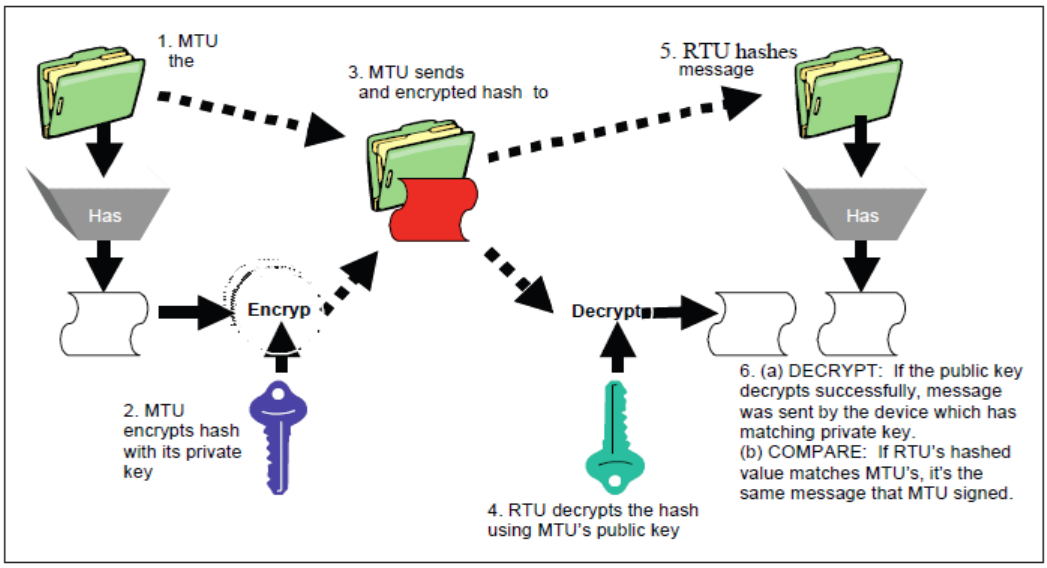
DNP3 user group had researched on two cryptographic techniques and tested it on a prototype which is presented here[134].

1. Authentication Octets: This is a digital signature based algorithm. Additional bytes are added to the packets which flow from the master to the remote station called as

[134] Sandip Patel, Information Science & Systems at Morgan State University, Baltimore, Ganesh D. Bhatt, Department of Information Science & Systems at Morgan State University, James H. Graham, Electrical and Computer Engineering at the University of Louisville, July 2009, "Improving the Cyber Security of SCADA Communication Networks". [Online] Available: http://portal.acm.org/citation.cfm?id=1538788.1538820

authentication octets. The purpose of adding these bytes is to authenticate the source. Figure 3-25 gives the schematic of how this algorithm is implemented. Authentication octets that are appended to the message are encrypted using the master's private key. Since the whole message is not encrypted, processing power is saved. The private/public key distribution is this algorithm is assumed to have been stored locally and hence there is no need for certificate authority. The message is also time stamped to avoid replay attacks. The RTU verifies with that the time of reception does not vary from the time of transmission beyond a specified range. At RTU the authentication objects is decrypted with the public key and compares it with the hash digest calculated by the separately by the remote station. If matched the data is unmodified during transit. The decryption technique makes sure that the message is from an authentic source. But this method does not protect from eavesdropping. But in SCADA network the requirement of having better authentication takes priority to eavesdropping[135].

Figure 3-25: Authentication Using Authentication Octets



In this technique both the devices have a shared key. Device which starts communication initiates a challenge to authenticate the other device. A challenge consists of a random number generated at the MTU and sent to the RTU. The RTU uses this random number and encrypts it with the shared key. The result message is sent to the MTU. The MTU decrypts using the shared key and checks if the decrypted result is same as the random number it originally generated. If it matches then RTU authenticated itself to the MTU else MTU terminates the connection. In order to verify authenticity after connection is established, e.g. during times when it receives a

[135] Sandip Patel, Information Science & Systems at Morgan State University, Baltimore, Ganesh D. Bhatt, Department of Information Science & Systems at Morgan State University, James H. Graham, Electrical and Computer Engineering at the University of Louisville, July 2009, "Improving the Cyber Security of SCADA Communication Networks". [Online] Available: http://portal.acm.org/citation.cfm?id=1538788.1538820

critical command for shut down or when values are out of typical range then RTU can again send the challenge to MTU[136].

The above two solutions were implemented and tested on a testbed at the University of Louisville; the testbed consisted of one master and 5 remote stations. 4 of the remote stations were connected to RTU through Ethernet while the 5th station was connected wirelessly. Snort intrusion detection sensors analyze the communication to extract relevant information to alert the administrator of unauthorized intrusions. The results showed in the table 3-32. Though authentication octets and challenge response takes comparatively more time they also provide enhance security features.

Table 3-34: Comparison of Security Approaches

	Total communication time (in milliseconds)
No Security	325
With SSL/TLS	373
With authentication Octets (software encryption)	2146
With authentication Octets (Hardware encryption)	764
Challenge response	446

3.5.2.4 Distributed Network Protocol Version 3 Security (DNPSec)

DNP user group started working on the Secure DNP3 from 2002. DNP3 protocol provides error detection mechanism and also uses sequence number fields to detect duplication of messages. Authentication, encryption or key management was not proposed in the initial version of the protocol. A new mechanism was added to the features of DNP3 present version of the protocol called DNPSecurity (DNPSec)[137] [138]. The goals of DNPSec are as follows:

- Provide Authentication and Integrity
- Low overhead.

---

[136] Sandip Patel, Information Science & Systems at Morgan State University, Baltimore, Ganesh D. Bhatt, Department of Information Science & Systems at Morgan State University, James H. Graham, Electrical and Computer Engineering at the University of Louisville, July 2009, "Improving the Cyber Security of SCADA Communication Networks". [Online] Available: http://portal.acm.org/citation.cfm?id=1538788.1538820

[137] Sandip Patel, Information Science & Systems at Morgan State University, Baltimore, Ganesh D. Bhatt, Department of Information Science & Systems at Morgan State University, James H. Graham, Electrical and Computer Engineering at the University of Louisville, July 2009, "Improving the Cyber Security of SCADA Communication Networks". [Online] Available: http://portal.acm.org/citation.cfm?id=1538788.1538820

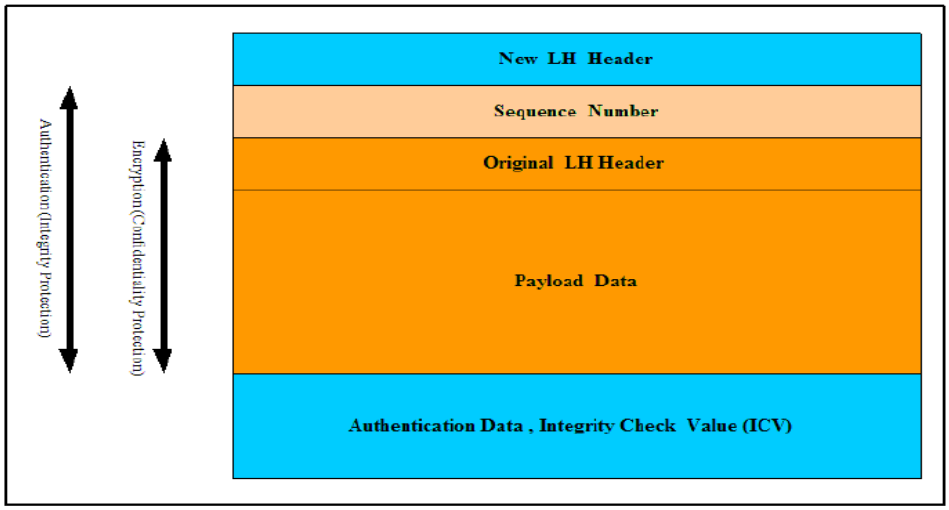
[138] Grant Gilchrist, PE, FnerNex Corporation, Okotoks, 2008," Secure Authentication for DNP3". [Online] Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4596147

- Support remote key management.
- Built into DNP at application layer.
- Compatible with all communication links supported by DNP.
- Make use of existing standards.[139]

There are two main components of the DNPSec. The first is the DNPSec structure to construct the frame and transfer data in secure mode between the Master and the Slave. The second is the key exchange established during the installation and connection setup between the Master and the Slave.

The figure below shows the new frame format for DNPSec.

Figure 3-26: DNP3 Protocol Structure



The protocol structure has a new header which is 4 bytes long. It contains the destination address, MH flag bit which indicates if the packet is from primary host or from the secondary host, the SK flag bit indicates if its new session key for the destination or it has to decrypt with the old session key and has another 14 bits which are reserved. The sequence number indicates the order of the message. It increments with every packet the master sends and cycles back at 232-1. When a new session key needs to be established, the present session must be terminated and a new frame with sequence number 0 and new session key must be sent. DNPSec maintains a session key life time period to keep track of the life span of a particular session key[140].

The original link header and payload is protected by encryption (excluding the CRC). It is composed of 264 bytes field containing, 8 link protocol data unit header bytes, 250 Transport Protocol Data Unit bytes, and 6 padding dummy bytes.

---

[139] http://www.nojapower.com.au/techdoc/docs/dnpsecurity.pdf

[140] http://www.acsac.org/2005/techblitz/majdalawieh.pdf

The authentication data field contains the integrity check value (ICV). This value is calculated with the sequence number field, original LH field and payload data fields. The function of this field is to provide integrity services and is done by using message authentication algorithm such as, HMAC-MD5-96 or HMAC-SHA-1-96. The steps for evaluation and comparison must be given in the integrity algorithm specification.

DNPSec Secure Authentication

DNP Secure Authentication is based on the IEC 62351 standards, and is designed to ensure that DNP outstations are communicating with an authorized master and vice versa.

Secure Authentication addresses the following threats:

- Spoofing (where a person or program masquerades as another)
- Modification (where data is modified in transit)
- Replay (where the same operation is replayed)
- Non-repudiation (identifying individual users, and ensuring only authorized users perform critical functions).

While DNP Secure Authentication is not designed to provide encryption or other security measures, such measures can be added outside the DNP protocol.

Basic Principles of DNPSec

DNP Secure Authentication adheres to the following principles:

- It uses authentication only, not encryption or other security measures. External measures such as bump in the wire link encryptors may be added independently if required.
- It is implemented at the application layer, as DNP must be used over a variety of different physical networks and it permits the possibility of protection against rogue applications
- It can be used in transmission direction, master-to-outstation or outstation-to-master.
- It is based on the common security concept of challenge and response as this places the responsibility for security on the device that requires authentication and it permits some communication to be left unsecured if desired.
- It allows for backwards tolerance, so that a secure device may communicate with a non-secure device.
- It follows the security principle of perfect forward secrecy. If a session key is compromised, this mechanism only puts data from that particular session at risk, and does not permit an attacker to authenticate data in future sessions.
- It allows multiple users of the system to be located at the site of the master, and it provides a method to authenticate each of the users separately.

- It allows outstations to limit access to certain functions, based on the identities of individual users[141].

Scenarios Where Authentication is Performed

- **Session Initialization:** When a master station initiates a DNP3 session with an outstation/slave, Secure DNP3 will authenticate both stations to prevent spoofing, replay and other attacks. A unique session key is generated and exchanged using pre-shared keys during this phase.
- **Periodic Authentication:** The master station and non-master/slave station will periodically verify their identity to prevent different attacks. The default interval for a periodic authentication is 20 minutes and the maximum is authentication every hour. A new session key is generated and exchanged while performing this periodic update.
- **Requests with Critical Function Codes:** Critical function codes can be the primary target of the attacker. Some example of the critical function codes are: write (FC 2), cold and warm restarts (FC 13, 14) etc. Authentication mechanism is used before responding to these critical function codes.
- **Vendor Specific:** Vendors can implement authentication requirements for other function codes or let end users to choose function codes that require authentication.

Modes of Authentication

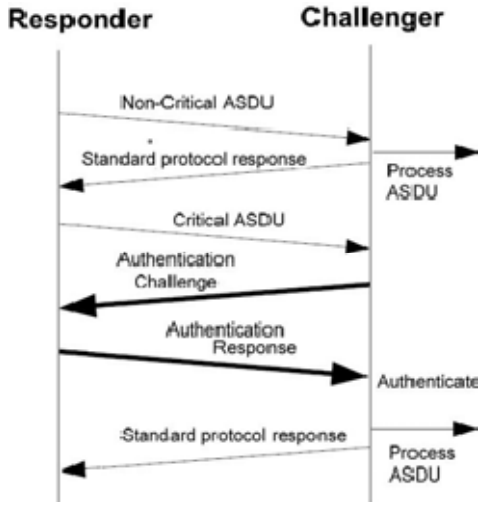
There are two modes of authentication in DNPSec as follows:

- Challenge Response
- Aggressive mode

Challenge Response: Critical messages received by a challenger require a challenge, unless aggressive mode is used. The challenge must complete successfully before the original message can be processed. Any application message can be challenged, but generally the outstation will challenge controls and other operations which may alter the outstation's state. Figure 3-27 illustrates the steps in Challenge Response mode.

[141] http://www.logica.com.au/file/16343

Figure 3-27: Message Sequence in Challenge Response

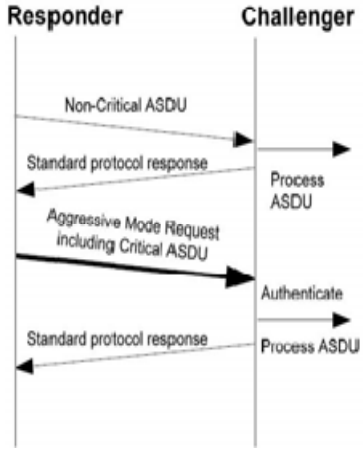


The challenge response works as follows:

- The responder sends the original critical application message to the challenger.
- The challenger replies with a challenge message containing some random challenge data.
- The responder sends a reply message containing an HMAC calculated on information from the original critical application message and the challenge message.
- If the exchange succeeds, the challenger may then process the original critical application message.

Aggressive mode: A responder sending a critical message may optionally anticipate the challenge by using aggressive mode. This reduces bandwidth, but at the same time also reduces security. Figure 3-28 illustrates the steps in Aggressive Mode.

Figure 3-28: Message Sequence in Aggressive Mode



The aggressive mode sequence is as follows:

- The responder sends the original critical application message to the challenger in aggressive mode, by including an HMAC value calculated on information from this critical application message and the most recent challenge message.
- If the aggressive mode HMAC is valid, the challenger may then process the original critical application message.

Key Management in DNPSec[142]

The key management operations in DNPSec are very simple to accommodate the static nature of the SCADA environment. They occur during the configuration of the Primary Master host, the Secondary Master host, and the Slaves to establish the initial connection between them; after the re-initialization of the Key Sequence Number (KSN) to generate and distribute a new key to the hosts; and after the timeout of the usage of the session key. Figure 3-29 demonstrates the key management operations in DNPSec.

The Master host generates and manages a secure database "M_Keydb" for the shared session keys with the Slaves. The master database consists of four fields as follows:

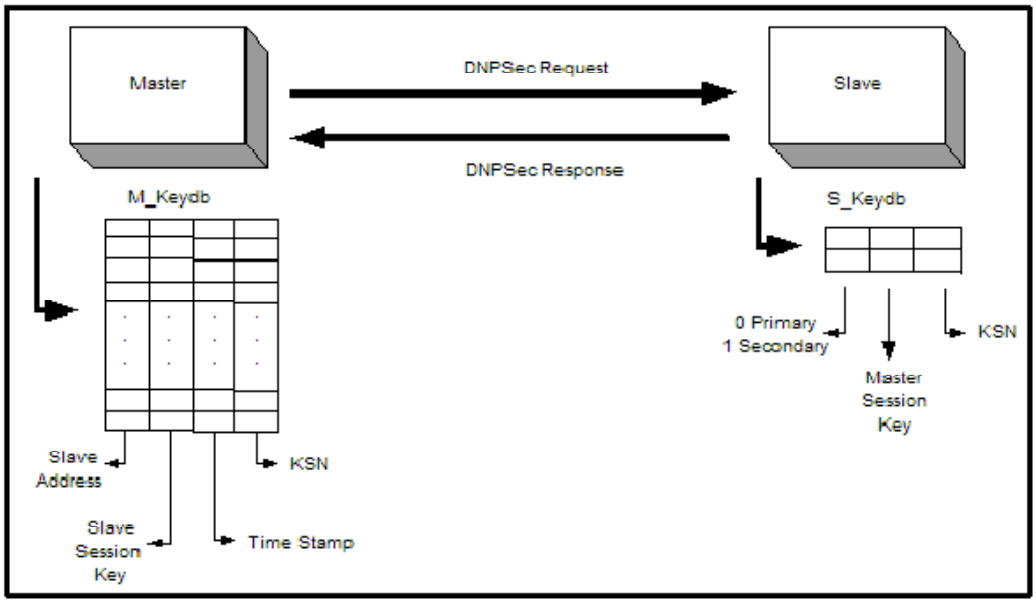
- Slave address used as an index key to the database
- Shared session key and time stamp used to limit the usage of the shared key for a certain pre-defined time period
- Key Sequence Number

The Master generates a unique session key when the old session key expired. Then, the new session key and new KSN will be inserted into the database.

The Slave needs to maintain two session keys, one for communicating with the Primary Master host and the other for the Secondary Master host. It manages a secure database "S_Keydb" for the shared session keys with the Master hosts. The slave database consists of three fields and two records: (0, Primary Master Session Key, Key Sequence Number and 1, Secondary Master Session Key, Key Sequence Number). The slave maintains the database by updating a new session key and a new KSN associated with the Master.

[142] http://www.acsac.org/2005/techblitz/majdalawieh.pdf

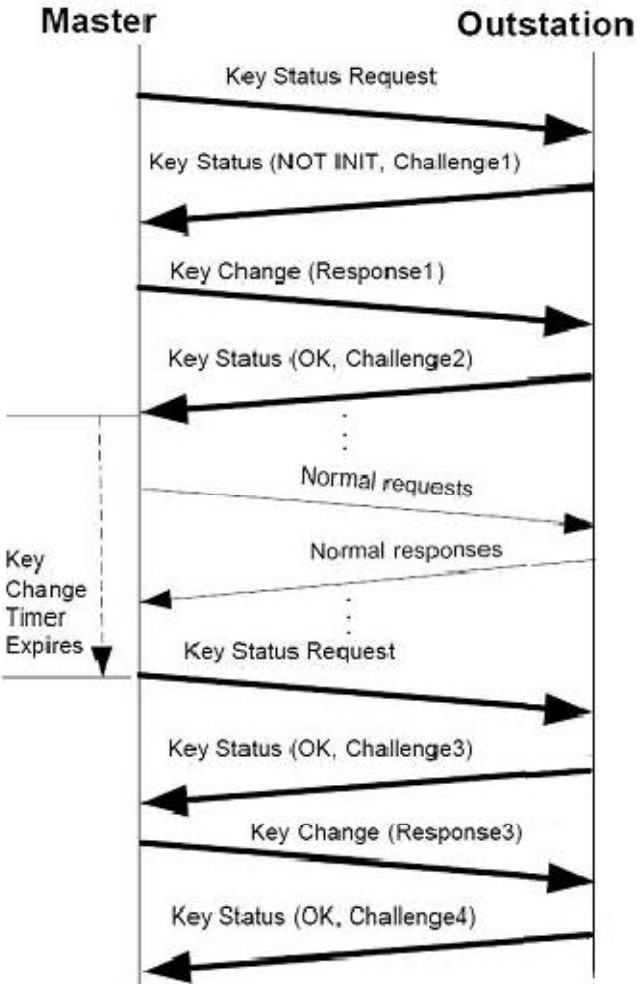
Figure 3-29: DNP3 Request/Response Link Communications



To start a session, the master generates a new set of random session keys, and downloads them to the outstation. Figure 3-30 illustrate the message sequences in the key management, which are performed as follows:

- The master sends a key status request to the outstation.
- The outstation replies with a key status message containing some random challenge data.
- The master generates two new random session keys and sends a key change message. The new session keys are wrapped using a key wrap algorithm and the update key.
- The outstation again replies with a key status message. If the exchange succeeded, the key status will indicate that the session keys are valid.

Figure 3-30: Message Sequence in Key Management



3.5.2.5 Comparisons of DNP3 Countermeasures

Table 3-35: Comparisons of DNP3 Countermeasures

SCADA/DNP3 Security Solutions	Advantages	Disadvantages
Wrapping DNP3 frame with SSL/TLS	• The IEC Technical Committee has accepted SSL/TLS as part of a security standard for their communication protocol • Freely available for all common OS	• Run only on a reliable transport protocol (TCP and not for UDP) • High performance cost • No non-repudiation services • Can't protect data before it is sent or after it arrives its

SCADA/DNP3 Security Solutions	Advantages	Disadvantages
	• Relatively mature	destination • Implementation of the protocol required understanding of the application, OS, and its specific system calls. • CA are rather expensive and not really compatible with each other
Wrapping DNP3 frame with IPSec	• Protection against DOS • Implemented by Operating Systems, Routers, etc. • Transparent to applications (below transport layer) • No need to upgrade applications	• Very complex and hard to implement • Higher performance cost • All devices shall support TCP and UDP communications on port number 20000
DNPSec	• End-to-End security at the application level to support any communication link • Protocol is simple eliminating the complexity of the key exchange and management issues • Implement it once for all communication networks	• Required some modification to the DNP3 Data Link Layer • Theoretical approach, needs to proof the concept (in going work)

3.5.2.6 Conclusion

DNP3 was not designed with security capabilities in mind. There are various techniques that be implemented to avoid the attacks on DNP3 protocol. Wrapping of DNP3 protocol structure in SSL/TLS layer or IPSEC layer will provide protection. However, this approach does not provide secure authentication. Another approach is by carrying out protocol enhancements with

authentication octets or via challenge response implementation to provide better authentication. Last approach discussed is the DNPSec framework to bring changes in the protocol packet structure to protect against attacks. The SCADA vendors can build such capabilities by utilizing the DNPSec framework with a minimum time and cost without a major impact on the systems components and the application supporting them. The DNPSec framework enables confidentiality, integrity, and authenticity in the DNP3. Such a framework requires some enhancements in the data structure of the DNP3 Data Link layer, without requiring modification to the Master Station and Substation devices and the applications supporting them. Confidentiality and integrity are achieved by encrypting frames between the Master and the Slaves using a common session key assigned at the setup time of the SCADA components. A new session key is established when the frame sequence number reaches the value 232 – 1 or when the time period for the use of the session key is expired. On comparing these approaches, DNPSec framework provides good security. Authentication is achieved by applying authentication techniques to assure that the sender of the frame is what it claims to be. Proof of concept by testing or simulation could be a future topic worth investigation.[143]

3.5.3 Countermeasures for Enhancing Modbus Security

The Modbus protocol was developed specifically for SCADA and has become the de facto industrial standard. Many vendors use this protocol and develop systems and produce equipment[144]. The vulnerabilities in Modbus Security Attacks can be classified into Serial Only Attacks, Serial and TCP Attacks and TCP only Attacks.

This section talks about the countermeasures that can be applied on Modbus protocol to provide enhanced security. The common security threats are as follows.

When the master sends a message to the field device, it needs to first authenticate the device from which it obtained the packet and then process the packet. Modbus protocol lacks this ability and hence middle man attacks can easily take place in Modbus. This middle man can bombard the slave units with messages and cause denial of service to the original legal master. The middle man can also carry out replay attacks i.e. capture the packets being sent and reuse them by fabricating it to do some other functions.

The best way to solve this issue is by repairing the Modbus protocol at its source. But this will require architecture modifications which are significant changes. Another way to approach this issue is by introducing smaller security mechanisms to protect against attacks.

Secure Modbus Protocol

A secure Modbus protocol must preserve confidentiality, integrity of the message. In order to satisfy these requirements unauthorized entity must not be allowed to access or modify the

---

[143] http://www.cs.louisville.edu/facilities/ISLab/tech%20papers/ISRL-04-01.pdf
[144] Modbus Organization, "Modbus Application Protocol Specification" [Online]
Available: http://www.modbus.org/docs/Modbus_Application_Protocol_V1_1b.pdf

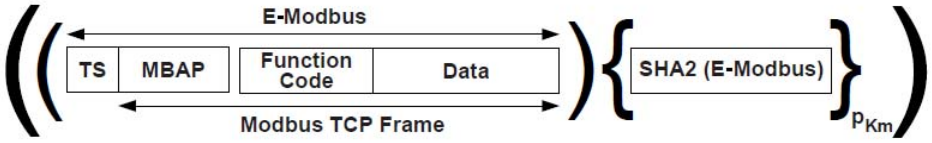
contents of the message. Also there should not be a middle man who can emulate the master or can negate a performed action.

In the original protocol, there is protocol data unit which is independent of the communication layer. When the Modbus messages are mapped to the structure of the bus or network it introduces additional fields. In the Modbus TCP protocol frame structure there is MBAP header where target address field in serial message packet is replaced by one-byte Unit Identifier in the MBAP Header. Error checking field is removed and length information is added. The length information is stored so that the receiving field device can identify the message boundaries when messages are broken down into packets. The Modbus packet can have variable sized or fixed size data fields. To identify if the entire message is received, in fixed size packets the information is inherent with the function codes. For function codes with variable data sizes there is a byte count field which transfers this information.

The secure architecture that is covered below is intended to satisfy the following security requirements[145].

1. Integrity of the data is maintained by using a secure hash algorithm. SHA2 (Secure Hash Algorithm) is used to generate the digest and transmitted along with the packet. The integrity is verified by computing the digest with the same algorithm and comparing it.
2. The above scheme does not prevent a middle man to create an own packet and send it to the field device. To avoid this kind of attack it is important to authenticate the master. Therefore a signature based scheme should be used. In this secure Modbus architecture RSA based signature algorithm is used. The master signs the digest with the private key and the field end device will use the public key to release the digest and check on authenticity. With this algorithm even availability will be fulfilled since only the owner with the specific private key can send the packet.
3. The above two schemes don't provide replay protection. Reason being the packet can be sniffed and obtained by a middle man. Hence a time stamp scheme is used which will help identify if the packet was sniffed or is the original packet. The packet structure incorporating time stamp is shown below in the figure 3-31.

Figure 3-31: Secure Modbus Application Data Unit



The Time Stamp (TS) is applied by the master device creating the packet including Mod bus Application Header (MBAP) and appended to the packet and sent to the destination. The

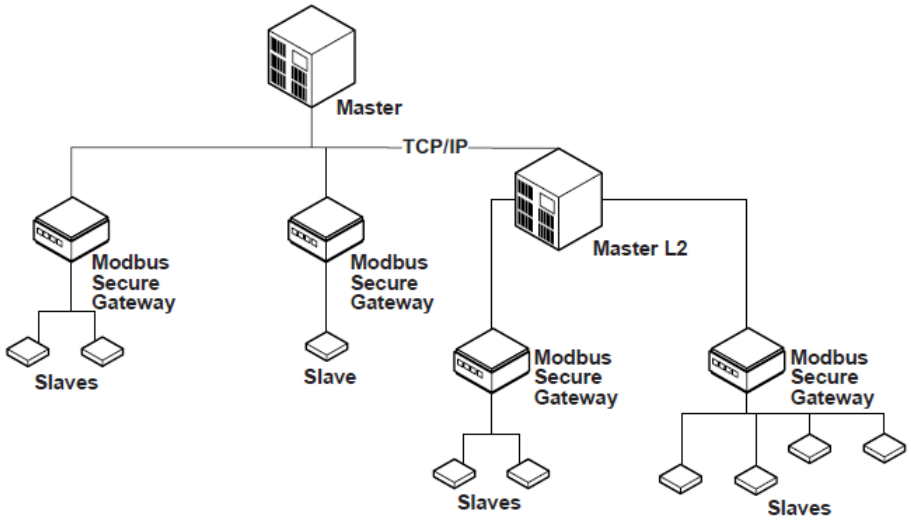
[145] Igor Nai Fovino, Andrea Carcano, Marcelo Masera and Alberto Trombetta, 2009, "Design and implementation of a secure Modbus protocol". [Online]
Available: http://www.springerlink.com/content/14h764755h412m15/

destination checks this packet along with a pre-defined and configured time interval. If the packet has reached within a time limit then it will be a valid packet. One way of implementing this is by using the Network Time Protocol (NTP). The NTP provides high precision for time interval by synchronizing the clocks of computer systems over packet switched, variable-latency data networks.

NTP requires additional equipment to be installed which is the NTP time server. This server provides reliable clock for all communicating devices.

Since Modbus is a protocol which was developed for old legacy systems in SCADA, applying the above stated extensions to this protocol requires more computing power at master and slave devices. In order to retrofit with the legacy systems a Modbus secure gateway was implemented which carries out the above procedures to make the packet transmission more secure. Figure 3-32 below presents a schematic diagram of the Modbus Secure Gateway.

Figure 3-32: Modbus Secure Gateway



This gateway is placed between the Modbus master and provides a multi-homed gateway with a TCP/IP interface connected on the master side and a set of point-to-point TCP or serial links connected to legacy slaves. Operation of the gateway is as follows.

When it receives a packet from the master side which flows to the slave, it carries out the following steps.

1. It discards any unauthenticated packets
2. Extracts the Modbus packet by implementing applying the SHA algorithm and checking it the packet has maintained its integrity.
3. It then forwards the packet to the particular slave destination

When it receives a packet from the slave device flowing towards the master it carries out the following steps

1. It creates the secure Modbus packet from the original Modbus packet
2. It signs the packet digest with its private key.
3. Sends the packet over to the master.

The steps to be followed when sending and verifying a secure Modbus packet is as follows

1. The master creates the packet (C) with function code required to carry out that command execution and the slave address. It also Time Stamps (TS) it. (Mreq)
2. Then it computes the digest, encrypts it with the private key (pKm) and sends the request to the slave or the gateway

   C = [TS|Modbus]{SHA2(TS|Modbus)}pKm
3. The gateway or slave verifies the packet by using public key (sKm)

   Mreq = {C}sKm

After verifying the benignity of the packet the slave address is read from the MBAP header and sent to the appropriate address. Same procedure is followed when the flow of packets take place other way round.

The following describes the secure survivable SCADA architecture to combat attacks wherein attacker is able to send a command packet to a slave. A command packet is illicit and a firewall will allow it to flow through. Hence when the packet is sent from an illicit source it will still flow through since it is a command packet. Therefore a solution to combat this is presented below.

1. The master composes the packet (C) normally (Mreq) and then the authenticity and integrity of the packet is maintained by using the RSA and SHA algorithms.
2. This packet is then sent to the filtering unit which validates by decrypting (Dec) the packet using the master's public key.

   Mreq = Dec {C, PKm}
3. The filtering unit analyzes the Modbus packet command and destination. If the combination is unusual and dangerous to the slave unit then it will add it into the dedicated stack of malformed packets.
4. If it is an untouched packet then it will authenticate by encrypting (Enc) the message with its own private key pKf and send it to the slave unit.

   MrF = Enc {Mr, pKf}
5. The slave (PLC) validates the filtered Modbus request (MrF) by the Filtering Unit's Public Key (PKf)

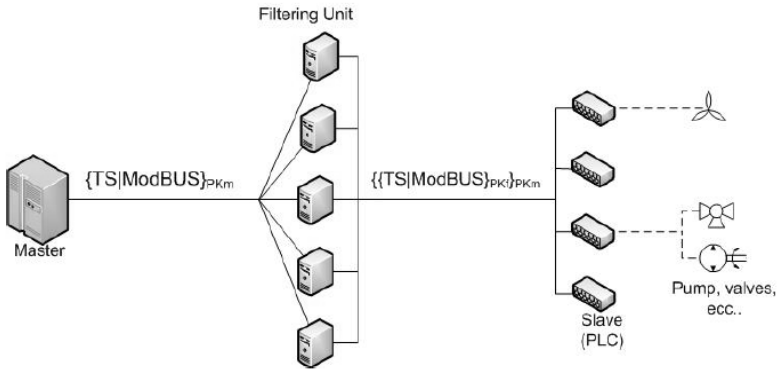
   Mr = Dec {MrF,PKf }
6. The slave validates the Modbus request (Mreq) with the Master's Public Key and executes the command

   Mreq = Dec {Mr,PKm}

But there is another security hole in this architecture. If the attacker takes control over both the filtering unit as well as the master then it can reach the slave unit. To avoid this scenario a concept of K-resilience is adopted. This means a mesh of N filtering units which a stronger operating system is deployed between the slave and master unit. The algorithm works in the following manner, when the packet from the master reaches the filtering units, it is sent to at least P filtering units. P should be greater than K.

Each filtering unit verifies the authenticity and sends it to the slave unit. If the slave unit at least obtains K number of packets of the same request then it will process the command. Now the attacker has to corrupt P filtering units to reach the slave. Figure 3-33 below shows in detail the proposed architecture.

Figure 3-33: High Level Secure Survivable Architecture



The proposed architecture will provide security is various areas. Does not allow corrupted packet command execution. Because of the signatures used it will provide data integrity. Prevent replay attacks with time stamps. Prevents a malicious master to send corrupted packets because of the filters used and also prevents the risk of the attacker reaching the slave through its K- resilience architecture.

The implementation of the prototype is as discussed below. Because of the physical architecture of SCADA the key exchange can be done manually to each system in a secure manner. There is no need for automatic key exchange. The RSA scheme was used for the signature based algorithm. Hence the signature will be applied on the Modbus packet and then encapsulated in the TCP packet. The basic communication layer between the operating system and the Modbus device is guaranteed by a socket, which manage the keep-alive messages, the TCPNODELAY and the TIME-OUT connections.

Components in the master slave unit should be designed for both functionalities of creating a Modbus packet and interpreting the received packet. The Modbus Stream adapter extracts the Modbus packet in the TCP packet and then authenticates it using RSA and checks its time stamp with the TS analyzer. The Modbus ADU Builder/Reader will check if the packet has a valid command to a valid address. It uses the message stack to store all the incoming messages and validate from the intrusion detection system.

3.6 Plug-in Hybrid Electric Vehicles

3.6.1 Introduction

The electric vehicle first made its appearance about a century ago, but it is only in recent years - months, to be more precise - that it has achieved breakthrough status as, the single-most important technological development having a positive impact on society today.

Climate change, over-dependence on fossil fuels, and the current economic crisis have combined to impact the automobile sector to a degree unforeseen, forcing technological innovation to direct its urgent attention toward the development of electric vehicles as an alternative means of transport, and a substitute for internal combustion engines.

It is certainly true that there exist pressures capable of driving the introduction of the PHEV forward, but technological advances are the factors that underpin and give coherence to its development. There are several progressive improvements being made in technology, materials, and power generation and supply, which will support the deployment and use of electric vehicles in the coming years. They include: advances in battery manufacture and electronics (particularly in terms of power); the development of new communication protocols; ever more efficient and flexible information technologies; the growth of renewable energy sources in the electrical energy generation mix; and the concept of smart grids focused on more efficient electricity distribution. All of these improvements are underscored by a much greater degree of passion and personal involvement by the end-user.

The Smart Grid will utilize Vehicle to Grid (V2G) which is one of the technological advances that will be used in making electric vehicles a viable mainstream option for prospective automobile customers. V2G will be a vital component for both the vehicle's owners and the energy providers because it will allow both parties to draw power from each other as needed. "Peak load leveling is a concept that allows V2G vehicles to provide power to help balance loads by "valley filling" (charging at night when demand is low) and "peak shaving" (sending power back to the grid when demand is high)."[146] V2G allows electric vehicle the capability to charge their fuel cells when energy demand is low while energy enables companies to draw power from the vehicles when there is a shortage of power.

Since most vehicles are parked an average of 95 percent of the time, their batteries could be used to let electricity flow from the car to the power lines and back, with a value to the utilities of up to $4,000 per year per car. Seeing that V2G follows the concept of peak load leveling, power consumers and providers can help each other reduce cost and improve overall effectiveness of power distribution. Even though there has been a significant amount of progress in solutions for the PEV related technological problems, other security issues associated with the technology and the data it will use remain to be dealt with.

---

[146] Woody, Todd. "PG&E's Battery Power Plans Could Jump Start Electric Car Market."

3.6.2 PHEV Charging and its Impact:

3.6.2.1 Battery Charging

Given that charging could be the action having the greatest impact on the electrical sector, there are various alternatives for affecting this. These include:

1. **Substitution:** This involves a rapid exchange of vehicles and/or batteries, and the subsequent charging of both in an offline mode. It would require sharing of cars (vehicle usage and substitution) and battery charging stations for quick and automated battery exchange.

2. **Direct Charging:** This includes regular charging points situated in car parks, shopping centers and residences, and providing battery recharge while the vehicle is parked. There also need to be fast-charging points that could quickly charge a battery in 10 to 15 minutes.[147]

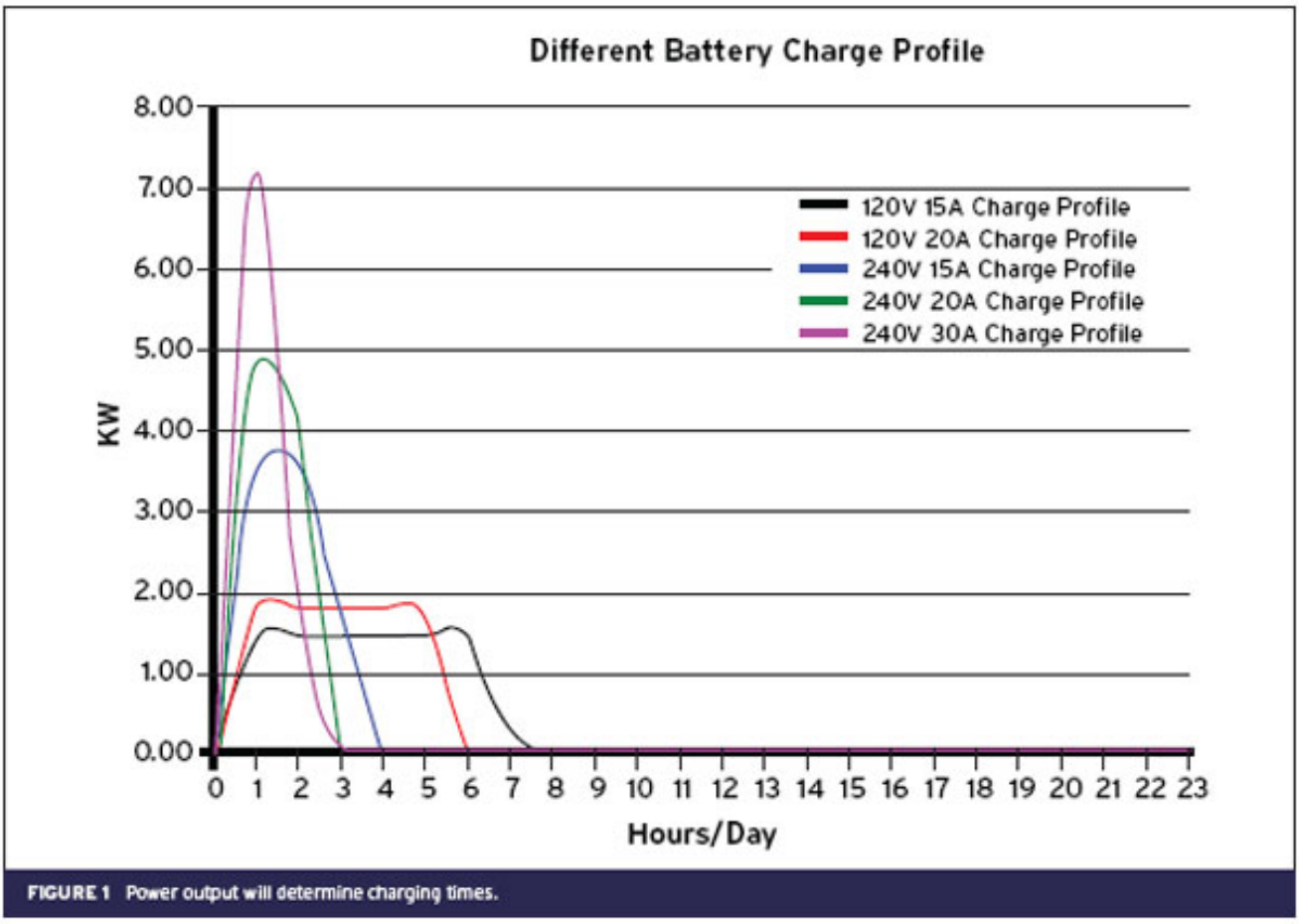
Offline charging could be the least invasive method given the current system of fuel distribution. A network of "electricity stations" (as opposed to petrol stations) could provide a dedicated system of energy generation in a given location. As for direct charging, given the itinerant nature of user demand and his or her expected freedom to choose a particular charging method or location, this introduces an element of greater uncertainty, and impact on the electricity grid, requiring a system that better adapts to the lifestyle of the user.

3.6.2.2 Direct Charging and Its Impact on the Electricity Grid

Direct charging depends on various factors - notably battery characteristics (directly related to vehicle performance) and the range of time spans chosen to carry out the recharge. Associated with these are other variables: charging voltage, mode (DC, single-phase AC, and three-phase AC) and the characteristics of the charging systems employed: technology, components and their location, connectors, insulation, and the power and control electronics. All of these variables will influence the charging times, and will vary according to the power input (more power, less time) as shown in the Figure 3-34 below. Therefore, depending on the kind of recharging, there will be an impact not only on the characteristics of the individual charging points but also on the supporting system.

[147] PHEVs on the Roll. http://www.mthink.com/utilities/phevs-are-roll. June 2008.

Figure 3-34: Power output determines the charging times

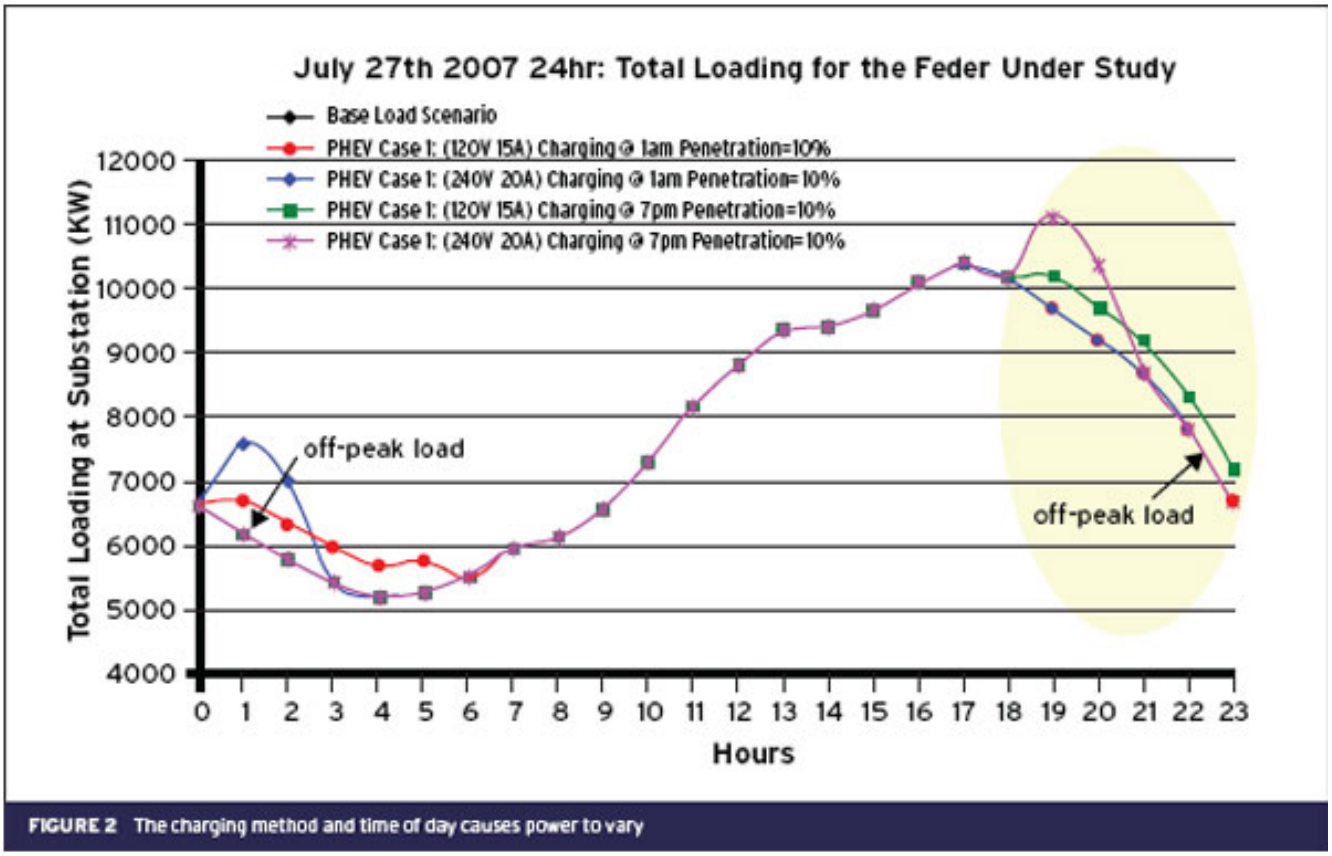


Based on the charging power input - and this is, of course, related to the methodology employed - it would be possible to fully recharge an EREV battery in about three hours. A fully charged battery would enable operation solely on electrical power for approximately 40 miles, a distance representing about 80 percent of daily car journeys based on the current averages.

For a scenario like this it would be possible to use a charging method of about 4 kilowatt/220 volts.

In terms of the instantaneous power available, the charging method will have a greater or lesser impact, particularly on the distribution assets, depending on how it is carried out. Figure 3-35 shows how the power varies according to the charging method and the time of day when it is in use, taking into account the daily energy demand curve. We can, therefore, identify different scenarios from the most favorable (slow charging at off-peak times) to the most unfavorable (fast charging at peak times). With the latter, we may find ourselves with distribution assets (e.g., transformers) incapable of supporting the heavy load of instant energy consumption.

Figure 3-35: Power Variance based on charging method and time.



It is necessary to link electric vehicle charging to the daily energy demand curve and instantaneous power availability in such a way that charging impacts the system as little as possible and maximizes the available energy resources. Ideally, there would be a move toward slow charging during off-peak periods. Furthermore, this kind of charging would not impact users as 90 percent of vehicles are not used between 11 a.m. and 6 p.m. Operating under such conditions would also permit the use of excess wind-generated power during off-peak times, enabling a clean locomotion device such as the PHEV to also use renewable (clean) energy as its primary source.

Smart charging would be capable of deciding when to charge in relation to different variables (for example, price and energy availability), and which energy sources to use (in-home energy storage, local and decoupled energy supply, plug-in to the distribution grid, etc.) Supporting the vehicle-to-grid (V2G) paradigm would enable managing and deciding not only when and how to best charge the vehicle, but also when to store energy in the vehicle battery that can later be returned to the grid for use in a local mode as a distributed energy source.

For all of this to be effective, a power and control electronics system (in both local and global mode), supported by information systems to manage those issues, is required. This will enable

the optimal charging process (avoiding peak times, and doing fast charging only when necessary) and an intelligent measuring and tariff system. The latter may be either managed by utilities through advanced meter management (AMM), or virtually through energy tariffs and physical economic transactions.

3.6.3 Security Issues and Counter Measures:

3.6.3.1 Privacy

PHEV will over load the smart gird when they are plugged-in for charging because the PHEVs move for place to place so the power requirements to the locations change. For example, there may be a city like Manhattan where more traffic flows in during peak office hours. If many PHEVs are plugged into the grid located at that point, at a time, it will overload the grid. To solve this problem the position of the PHEVs should be monitored all the time. Due to the constant monitoring of the PHEVs, there is no privacy to one's individual freedom since his PHEV location is being monitored all the time. If someone breaks into the monitoring system, he can get access to this information.

3.6.3.2 Secure Payment

A very important element to the smart grid is a payment system which works reliably and secure, and which protects both the end-user as well as the provider. There are good reasons to prefer electronic payment systems rather than sticking to cash payments, such as reduced revenue collection costs and a reduce of losses, enhance customer satisfaction, improved services and operational efficiency as well as more flexible pricing strategies. One type of solution is to use credit cards. However credit card systems do have problems as well. For example, transaction needs to be protected so that an individual's information is not revealed to third parties. Another approach would be to adopt Integrated Transportation Payment Systems (ITPS. Unfortunately, there are also examples of serious shortcomings of today's ITPS. Existing systems do not have mechanisms protecting their security and especially the privacy of their users. One problem is that some systems deploy cryptographically weak proprietary primitives. Currently e-cash protocols have been extensively studied. The study shows that it is possible to construct secure off-line payment that protect the anonymity of honest users but is nevertheless able to disclose their identities as soon as they try to cheat the system[148].

Potential attackers can be categorized as a small set of individuals, commercial companies, and government institutions. Typically regular individuals will attack the system to acquire private sensitive information in order to track other individuals. Individuals will also attack the system because they are curious or because they see it to be a challenge. On the other hand commercial companies will generate user profiles to increase their revenue. They will usually respect legal restrictions but they will also exploit legal loopholes. And finally government institutions will have extensive power and they might even be able to define the legal environment. Therefore it

---

[148] Christof Paar, Andy Rupp, Kai Schramm, André Weimerskirch, and Wayne Burleson. Securing Green Cars: IT Security in Next-Generation Electric Vehicle Systems. http://www.crypto.ruhr-uni-bochum.de/imperia/md/content/texte/publications/conferences/it_security_for_electric_vehicles.pdf. University of Massachusetts, Amherst.

is important to define a legal framework to account for companies and government institutions, and define technical solutions that account for individual attackers.

Privacy is a challenging problem, since it involves cryptographic theory, engineering, policy and sociology. In order to enable a deployment, adequate security and privacy mechanisms must be a requirement. To prevent malicious actions by attackers some form of IT security need to be introduced to systems. Such methods range from cryptographic mechanisms, to secure and privacy-preserving payment systems to a critical infrastructure interpretation of the electric car charging network. This should lead us towards addressing the security problems.

3.6.3.3 Smart Metering

Electricity has no physical form, it can neither be visible nor has any physical weight, and therefore it is very difficult to accurately measure electricity. Knowing this about electricity, that we can make a claim that there will be an inherent incentive for all parties involved in the production and consumption of electricity to be dishonest when reporting the sale of and purchasing of electricity. The owner of the PEV would want to report less electricity than what was actually delivered to the PEV's batteries, and the energy provider would want to charge for more energy than what was actually delivered. Even worse than these two would be a third party or middle man, such as a charging station, which would be able to cheat both the energy providers and the owners of the PEV. This can all be done if we are not careful in securing the smart meter from tampering.

In order to provide strong protection to this new technology, three defensive techniques are required, which are based on embedded security technologies.

First, the metering data which records the electric energy delivered should be signed using a digital signature within the charging station. A digital signature assures that the data cannot be manipulated later unless an attacker has access to the private cryptographic signature key. Applicable signature algorithms include DSA, RSA or ECDSA, (as specified by The US Federal Information Processing Standard). These algorithms are computationally demanding, but given that a signature has to be derived only every few seconds, even inexpensive embedded CPUs provide sufficient computational resources.

The second crucial component is that the software or hardware module which computes the digital signature is closely linked to the actual metering device. Otherwise, a potential attack could be that the data from the analog metering IC is manipulated as it is being sent to the digital signature module. Even if both ICs are placed on the same circuit board within the "pump", attacks are possible by manipulating bus data (Such "modchip" attacks are common against video game consoles as the Xbox). In order to prevent the attack, the metering circuit has to be either in the same IC as the digital signature algorithm, or both modules have to be placed in tamper- resistant housing which detects manipulations. Interestingly, such an approach shows similarities to anti-counterfeiting technologies in which products or spare parts are equipped with electronic tags (e.g., RFID tags) which authenticate the part and are physically connected to the target in a tamper-resistance manner.

The third security component assures that the data is hidden during transmission. Even though not absolutely necessary, in most scenarios it will be highly desirable that the metered data is not only protected with a digital signature against alterations, but also encrypted as it is being transmitted, e.g., to the charging station display or to the utility company. In order to establish such a confidential communication channel, symmetric algorithms like the Advanced Encryption Standard (AES) can be used. If payment information is to be transmitted too, e.g., credit card numbers, encryption will be a crucial requirement.

Both the digital signature and the symmetric encryption rely on cryptographic keys which must be stored securely within the metering station. There are established methods for achieving secure key storage. One of the more challenging aspects of the system will be the key management. Given the distributed nature of the system, using a public-key infrastructure (PKI) seems like a promising approach. A PKI allows to exchange the public keys needed for digital signatures and to compute the symmetric session keys.

3.6.3.4 Critical Infrastructure & Physical Security

Critical Infrastructures are defined as "complex highly interdependent systems, networks and assets that provide the services essential for a modern society" [PEV-1]. These critical infrastructures are organized into seventeen sectors, including energy, and transportation, which must be protected against malicious attacks. When the PEV's become the norm and the combustion engine is a thing of the past. The link between the energy and transportation critical infrastructure will become tightly intertwined. Any malicious attack made against either one of these two critical infrastructures could potentially pose as a threat to the security of these two infrastructures, specifically in the areas of traffic management, and payments for services rendered, specifically pertaining to charging of a PEV.4 Since the link between these two critical infrastructures is in uncharted territory for both the energy and transportation critical infrastructure sectors, studies will need to be made in order to better understand the impacts of such a close relationship between the two sectors. If a malicious attack were to penetrate the defenses of either the energy or the transportation critical infrastructure, it would be devastation to both critical infrastructures, monetarily and physically. Many businesses will not be able to operate without the ability to charge their vehicles. Traffic management will also become a problem, and can potentially lead to physical harm to individuals. Because of the severity of the problems that can be caused by a malicious attack, the Department of Defense should be an active participant in the security of the energy and transportations sectors of the critical infrastructures.

Physical Security of the equipment is also a very important to the security of PEV's. If an individual is given the chance to take something without paying for it, most of the time that individual will take the opportunity. In this case we are talking about electricity. The Smart chargers will need to be secure enough so that a potential attacker cannot hack the smart charger for a PEV to provide their PEV with free electricity. There also might be attackers out there that are not only looking for free electricity; instead they want to be able to obtain sensitive information from the smart charging of the current owner or previous owners of the smart charging device. This potential security threat can be solved by using encryption and

Trusted Platform Modules (TPM), in order to store the encryption keys on the tamper proof module. Sometimes attackers are not just looking to steel information or energy; sometimes they are looking to cause physical harm to the owner of the PEV. If a battery is overcharged there is a possibility that the battery will explode and cause physical harm to anyone in the vicinity of the explosion. The solution to such a problem should be multi-faceted. The manufactures of the battery should include circuitry to not allow over charging of their batteries and the smart meter should make sure that over charging of a battery is not allowed. Another place that an attacker can cause mischief is at a charging station for a PEV's, by either skewing the amount of energy purchased or by stealing credit card numbers via card skimmers. Particular care has to be taken when dealing with the physical security of the hardware that involves PEVs.

Successful integration of PEVs into the Smart Grid depends on overcoming the security challenges of "Secure Payment and Privacy, Smart Metering, and the Critical Infrastructure and Physical Security."

3.6.4 Tamper-resistant

PHEV's devices which are used for metering the power usage, communicating with the towers and other PHEVs must be electronically intelligent, tamper-proof electronics, and backup power. Why are anti-tampering methods important in the United States? At increasingly high electricity rates, a 4% loss is enough to get the utilities' attention. But, even more important, stolen power is the most common power source for illegal marijuana "grow houses." The power bill for such houses in urban areas can easily hit $10,000 a month, and stealing power from nearby power lines is a convenient way to get it. This could happen in the PHEV's billing system also if not tamper-proof anyone who knows little about how this device works can use their knowledge to send false information about the power usage from the PHEV and reduce the bill[149].

3.6.5 Communication

The PHEVs use cellular network for communication but there are many vulnerabilities in this network that can be used as a means of getting access into the system or sending wrong information, attacking the system etc. The types of attacks are middle-man-attack, spoofing, fingering and many more.

3.6.6 Security Issues with Networking

The new trend in the networking world is Cross Platform/Network Systems (CPS). It is one new method that even the smart grid data transmissions such as the PHEVs would rely on. This system has myriad benefits but along with them, there are some security issues cited as well.

We categorize the security issues based on three types of attacks. Traditional attacks in the Internet (TA), newly identified attacks in CPS (NA) and cross-platform attacks (CPA). The cross platform networking system are used in PHEV communication system because the information

[149] Electronic Strategy Designs News. http://www.edn.com/article/CA6643364.html

from the PHEV must be sent to different systems which rely on different networks such as SCADA for power management, DR for pricing information etc. The Internet 3G cross Network will be the primary channel through which the PHEV will send its information to other systems. The tables below table 6.1 and table 6.2 contain varies attack methods and their countermeasures for cross platform networking systems and 3G Cross networks.

3.6.6.1 Cross Platform/Networking Systems

Table 3-34: Categories of Attacks in CPS

Attack Categories	Countermeasures
Traditional Attacks(TA) TA1: Eavesdropping; TA2: Hijacking/Man-in-the-middle; TA3: Masquerading; TA4: Tampering with Message Bodies; TA5: Denial of Service	C1: Authentication and Authorization C2: Encryption C3: Integrity protection C4: Firewall
New Defined Attacks in CPS (NA) NA1: Malicious Codec Change(MCC) attack; NA2: Malicious-Formatted Packet Flooding(MFPF) attack; NA3: Cross-Platform Denial of Service (CPDoS) attack; NA4: Malicious Code injection and traverse attack	C-NA1: Countermeasure to MCC attack C-NA2: Countermeasure to MFPF attack C-NA3: Countermeasure to CPDoS attack C-NA4: Wireless station hardening and wireless network monitoring based defense
Cross-platform Attacks (CPS) CPA1: Power Management attack; CPA2: Traffic Analysis Attack; CPA3: Packet modification deletion/replay attack	C-PA1: Synchronization and encryption based defense C-PA2: Hiding explicit and implicit identifiers C-CPA3: Cryptographic approaches

3.6.6.2 Internet 3G Cross Network

Table 3-35: Attacks and Counter measures on Internet 3G Cross Networks

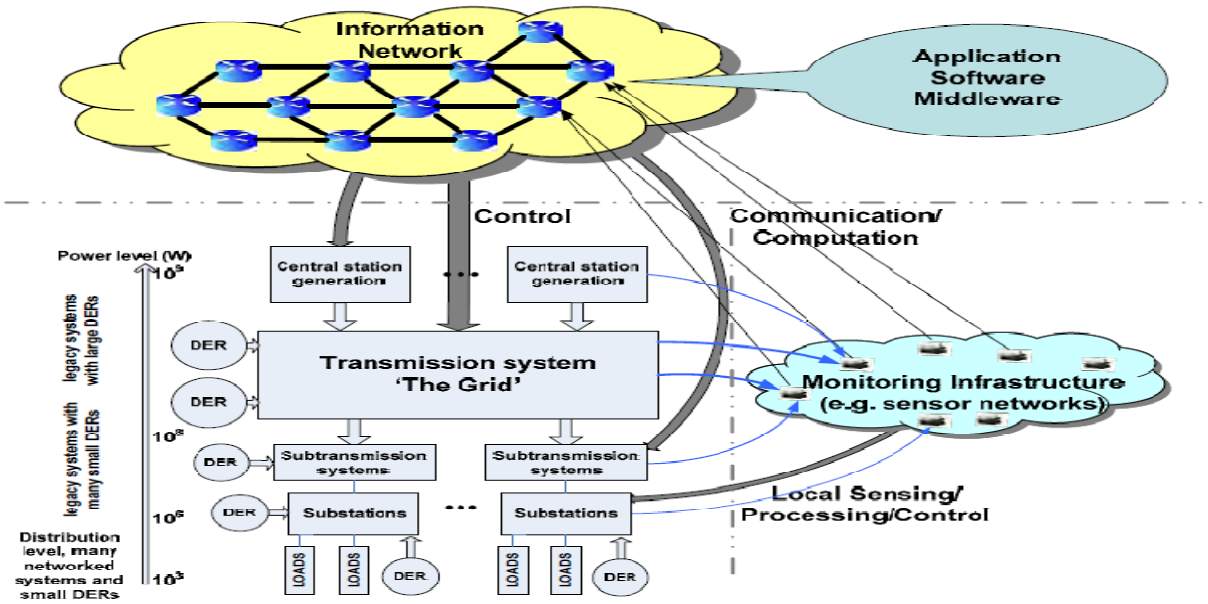
Cross-Protocol(Internet 3G)		Key Operation	Attacks	Countermeasures
Application layer	SIP <-> ISUP	Signaling Translation -Registration -Session Initiation -Session Termination	TA1: Eavesdropping (Include User Account. Network Topology. Etc.) TA2: Hijacking/Man in the Middle (Redirect Call) Ta3: Masquerading (Fake Registration/Invitation/Teardown, etc.) TA4: Tempering with SIP Headers NA3: Cross Platform Dos	C1: Authentication(HTTP Digest, MD5) C2: Encryption (SIPS, SSL, TLS, PKI) C3: Integrity Protection and Sequence Number Check C4: Firewall C-NA3: Countermeasure to NA3
	SDP<-> H.245	Signaling Translation -Capability Agreement -Codec Selection -Codec Modification	TA1: Eavesdropping TA4: Tempering with SDP Bodies (Include Capability Set, Destination Address and Port, etc.) NA1: Malicious Codec Change	C2: Encryption (SSL, TLS, PKI) C3: Integrity Protection and Sequence Number Check C1: Codec Modification C-NA1: Countermeasure to NA1
	RTP/UDP <-> h.223	Media Transformation	TA1:Eavesdropping TA5: Media Packets flooding (Dos, waste resource if transformation module of cross-platform gateway) NA3:CPDoS	C2:Encryption (SRTP) [21] C3:Packets Content, Timestamp and Sequence Check C-NA3:Coutermeasure to NA3
	G.7xx<->AMR	Media Transcoding -Audio Decode -Audio Encode -Video Spatial transcoding -Video Temporal transcoding	NA2: Malicious-formatted packet flooding	C-NA2:Coutermeasure to NA2

Cross-Protocol(Internet 3G)		Key Operation	Attacks	Countermeasures
Transport Layer	TCP/UDP<-> SCCP	Connection Control -Connection oriented Establishment -Connectionless oriented Establishment -Connection Maintenance	TA1:Eavesdropping TA5:UDP request/response flooding TA2:TCP session Hijacking TCP SYN/ACK flooding TA4: Tampering Message (modification/deletion/replay)	C1: Authentication C2: Encryption (IPSec, SSL, TLS, PKI) C3:Integrity protection C4:Firewall (TCP Session Control)
Network Layer	IP <-> MTP3	Route Control	TA1: Eavesdropping TA2: Hijacking/Man in the Middle(ARP spoofing, ICMP redirection, Malicious Routing Node/Signaling Node) TA4: Tampering Message (modification/deletion/replay) TA5: Ping flooding, ICMP unreachable Storm	C1: Authentication (802.1x, AH/ESP) C2:Encryption (IPSec, PKI) C4: Firewall(IP and Port Restricted) C3: Integrity protection and Sequence Number Check
Link Layer	802.3<->MTP2	Link Control	TA5: DoS (MAC/CAM flooding DHCP flooding) TA2: Hijacking/Man in the Middle	C1:L2 Authentication(802.1X) C4:Firewall (DHCP and MAC/CAM Restricted)

3.7 Distributed Energy Resources (DER)

A conceptual architecture of the smart grid depicted in figure 3-36 below, illustrates a synergy of computing and physical resources, and envisions a trustworthy middleware providing services to grid applications through message passing and transactions. The architecture also depicts a power system infrastructure operating on multiple spatial and temporal scales, which is a key in supporting the growing penetration of distributed energy resources. There will also be thousands of sensors and actuators that will be connected to the grid and to its supporting information network. Energy generation, transmission, and distribution will be controlled by a new generation of cyber-enabled and cyber-secure energy management systems (EMS) with a supervisory control and data acquisition (SCADA) front end.

Figure 3-36: Architecture for Proposed Integrated Smart Grid Systems150



The information network will merge the capabilities of traditional EMS and SCADA with the next generation of substation automation solutions. It will;

1. Enable multi-scale networked sensing and processing,
2. Allow timely information exchange across the grid and
3. Facilitate the closing of a large number of control loops in real - time. This will ensure the responsiveness of the command and control infrastructure in achieving overall system reliability and performance objectives.

The benefits from the Smart Grid can be categorized by the three primary stakeholder groups:

- Consumers can balance their energy consumption with the real time supply of energy. Variable pricing will provide consumer incentives to install their own infrastructure that supports the Smart Grid. Smart grid information infrastructure will support additional services not available today.
- Utilities. Utilities can provide more reliable energy, particularly during challenging emergency conditions, while managing their costs more effectively through efficiency and information.

---

[150] Power Systems Engineering Research Center. http://www.pserc.wisc.edu/ecow/get/publicatio/2009public/pserc_smart_grid_white_paper_march_2009_adobe7.pdf March 2008.

- Society. Society benefits from more reliable power for governmental services, businesses, and consumers sensitive to power outage. Renewable energy, increased efficiencies, and PHEV support will reduce environmental costs, including carbon footprint.

Smart Grid, particularly with a full-deployment of smart meters and expected market penetrations of advanced Distribution Automation (DA) devices, PCD and DER, adds a massive volume of data that will need to be managed effectively. The data includes asset installation location and other attributes, device configuration, equipment performance, inspection and maintenance history and pending work orders as well as measurements and controls of Smart Grid devices. Effective management of the data throughout the utility enterprise is essential to reducing Smart Grid/AMI deployment costs, sustaining benefits, and perhaps more importantly manage business continuity risks from deploying far-reaching and transformational technologies like Smart Meter and Smart Grid.

To prepare for the inrush of Smart Grid data that would be generated by the integration of DER into the smart grid, even at the pilot stage, the utility should develop holistic enterprise architecture and integration plans to cover the following, equally important, four areas of need in order of implementation timing:

1. Deployment of Smart Grid systems and devices, including smart meter and in-premise PCD as well as advanced system automation equipment – to ensure efficient installation, and timely and accurate asset data capture during installation.
2. Management of the collected data on Smart Grid asset, system and device configurations – to ensure quality control of the data and that the systems and applications that need the data are updated timely.
3. Operation and maintenance of the Smart Grid assets, including hardware, firmware, and software – to ensure that the system, equipment and devices will be properly maintained from day one.
4. Management and use of data collected from the Smart Grid systems to improve the utility business, including operation efficiency, capital planning and capacity utilization, T&D system and energy efficiency, and customer service.

With all this taken care of, the questions that arise next are: Are the utility's current cyber security and information protection policies, guidelines, and processes adequate in light of the expanded distributed command and control capabilities as well as the detailed customer usage information data that are becoming available? Do existing system and prospect technology products, and their implementations and integration; provide adequate security measures in their products?

3.7.1 Physical Security

Smart Grid will derive its electricity from a combination of renewable and conventional energy sources. Physically, fortifying Smart Grid's critical infrastructure is a new and daunting challenge because renewable energy facilities in particular spread out over vast distances. Wind is generally viewed as the most likely renewable incremental electricity source over the next

several decades. The American Wind Energy Association reports utility-scale turbines for land-based wind installations come with rotor diameters ranging up to 300 feet. DOE indicates typical turbine spacing is five to ten rotor diameters apart, leading to well over a half mile between turbines. DOE concludes generating 20% of electricity with land-based wind installations would demand at least 20,000 square miles. By comparison, all US nuclear power plants, which produce roughly 20% of power, occupy only 115 square miles.

Smart Grid will require a "backbone" of extra-high-voltage transmission lines, which carry between 345 and 765 kilovolts (kV) of electricity. These power lines will increase the capacity, efficiency, and reliability of the grid. To the extent wind is the source of new generation, tens of thousands of miles of new transmission lines and their support structures will need to be built. Most potential sites for large-scale wind (and solar) farms are removed from population centers. It is estimated that this is going to require literally thousands and thousands of miles of new transmission.

Opinions and Estimates:

A well-marketed wind energy plan, calls for 100,000 wind turbines and 40,000 miles of new high-voltage (>230kV) transmission lines to be built in the Great Plains Region. The physical exposure of this infrastructure could compromise system security, however, as the bulk of new lines will need to be overhead transmission. Experts have suggested burying lines underground will improve Smart Grid's security. Unfortunately, burying power lines is generally not feasible, as it makes them more susceptible to weather damage and slows repair time. Further, a study by the Edison Electric Institute (EEI) indicated putting power lines underground would cost about $1 million a mile compared with $100,000 to install overhead lines. [151]

3.7.2 Cyber Security

Distributed energy has turned out to be the new trend of the environment conscious authorities and the citizens as well. The outcome of which has come in the form of an urge to integrate Distributed Energy Resources as a means to generate energy for the rising Smart Grid technology. But this integration brings with it a lot of security concerns that could violate the basic working principles and so need to be taken care of as efficiently as possible. Most of the DER security concerns are covered in multiple sections in this chapter.

If the energy is being generated from a vast generation site at a far of location, the amount of energy being generated and transmitted can be monitored by having a good metering and monitoring system. This method of energy generation is well taken care of as there are authorized personnel involved in these kinds of transmissions.

---

[151] Jude Clemente, "The Security Vulnerabilities of Smart Grid".

http://www.ensec.org/index.php?option=com_content&view=article&id=198:the-security-vulnerabilities-of-smart-grid&catid=96:content&Itemid=345 Journal of Energy Security, April 2009.

But with the dawn of technology, citizens are also getting environment conscious and building solar panels on roof tops, backyards, vacant land by their property and any open space available. By doing so they are generating some amount of energy themselves, this energy needs to be accounted for. The advent of smart grid brings along with it features of bi-directional communication between the customer and the vendor, a means by which the customer can send any extra energy being generated to a distribution point so that it could be directed as supply to another line. This sure is a very advanced and well thought of aspect but it brings with it a lot of security issues as well. The AMI is a device that ultimately monitors the amount of energy being consumed or even generated; it keeps track of the entire household consumption and generation information as such. But the drawbacks arise due to it being easily accessible as it is placed at home, within the customers' reach. Due to this many security issues can arise, some of them are listed below;

1. ***Cheating Customer:*** The customer at an endpoint would attack to achieve the goal of reduced cost of electric and/or natural gas use. They would use information freely available from the AMI meter vendor or a standard associated with AMI meters to reset the meter and reprogram it to report false information. If the information is not freely available, the attacker would reverse-engineer a meter to develop a way to modify it. This is very similar to the many cable modem attacks that are openly available. Either the configuration settings from the utility or the actual firmware controlling the operation of the meter would be modified in this attack.
2. ***Repudiation:*** People may generate energy from their personal solar panels, but would not want to give the right information, in which case, they may resort to modifying the AMI data and thus refuse to acknowledge an action that took place. People may physically intrude into AMI system components like Smart Meter to perform unauthorized actions. This is one big threat involved in a person having the freedom to generate energy using DERs.
3. ***Insider Attack:*** The insider attack would take advantage of access to systems at the opposite end from the customer endpoint. The systems that the insider may be able to access include the AMI head-end, the system from which it gets pricing information and the network infrastructure supporting both of those systems. Which cyber-effect an insider uses would depend upon their access to these systems. One with solar panels at his place or other DERs may use the system which generates the pricing information and try to tamper with it.
4. ***Unauthorized Access from Customer Endpoint:*** There is a potential for AMI to allow access to the bulk electric grid from the residential or small business customer endpoint. The adversary can suborn the customer endpoint, crack wireless communications between the AMI meter and other endpoint equipment, or crack wireless communications from the AMI meter to the local concentrator. These attacks will expose the head end equipment and systems to which the head end are connected. Certain configurations would allow an attacker to affect the bulk electric grid.

5. ***PHEV charge points:*** Such issues would also rise regarding the usage and charging of PHEVs. Customers, who own the PHEVs would charge it at their own expense and if they have distributed energy sources, would also provide a charging point to other customers. But how would they keep track of a right billing and payment technique is another area of concern.

Thus we see how the generation of energy using distributed energy resources though does not directly pose a threat but it sure reflects on all its interrelated components, posing vulnerabilities in what should have been a secure grid technique. The freedom and ease of energy generation through distributed energy sources such as wind power, solar power, fuel cells etc. and the feature of bi-directional flow of energy in the new smart gird technology need to be given thought about how to avoid the threats discovered in this region so far.

CHAPTER 4:
Identifying And Categorizing Research And Development Issues For Cyber Security In The Smart Grid

4.1 Introduction

This chapter is about Potential Research and Development (R&D) Topics for Smart Grid Cyber Security as well as categorizing the R&D topics into confidential and non-confidential.

The best practices discussed in chapter 3, provides solutions to several threats, but there were still areas where these solutions are not adequate. This chapter discusses a number of potential research and development topics for Smart Grid cyber security. Another intent of this chapter, is to discuss whether the processes for conducting a specific R&D in smart grid cyber security and the results thereof should be publicly disseminated or not.

Basic research delves into scientific principles and applied research which uses basic research to better human lives. R&D can be theoretical, experimental, long-term (5-10 yrs), or short-term (less than 5 yrs). This chapter does not specify which of the above categories each research problem falls into. Additionally, in many cases the terms research and development are used interchangeably.

The potential research topics are organized as follows:

1. **General topics**

   This covers general topics which could be applied to different domains of the Smart Grid, including trust management, cost-effective tamper-resistance and tamper-evident systems, information handling practices, patches, and firmware updates as well as Role-Base Access Control (RBAC).

2. **Potential research topics in Cryptography**

   This section is intended to cover the potential R&D topics with respect to Cryptography and Key Management, which could be implemented in the Smart Grid, such as Public Key Infrastructure (PKI), key management alternatives such as identity based encryption (IBE), Low power encryption techniques, etc.

3. **Specific domain topics**

   These research areas cover Neighborhood Area Networks (NANs), Home Area Networks (HANs), Residential Gateways, Demand Response (DR), Supervisory Control and Data Acquisition (SCADA), Distributed Network Protocols (DNP3), Advanced Metering Infrastructure (AMI) as well as Plug-in Hybrid Electric Vehicles (PHEVs). These topics are grouped together because those domains are related to each other.

4. **Wireless communication security topics**

These are topics which are related to networking but that are not grouped into the first three categories.

4.2 General Research Topics

4.2.1 Cost Effective Tamper-Resistance & Tamper-Evidence

Tamper resistance refers to a process, mechanism or device that protects a system from various kinds of tampering, such as unauthorized accesses, unintended information altering and stealing. Tamper evidence refers to a process, mechanism or device that makes the tampering to protected resources/objects become detected. Tamper resistance must be implemented in such a way that the devices, such as meters and other IEDs are not easily tampered by either local or remote attacks, and by any physical attacks. For example, the devices might be swapped with a fraudulent one. Also, if the devices are attacked by any means, there must be some kind of evidence to indicate that the device has been manipulated. Thus, tamper evidence is also critical in Smart Grid systems. Security mechanisms, such as cryptography, Intrusion Detection Systems (IDS), or firewalls can help mitigate the risks of being attacked by an adversary. However, since the Smart Grid is required to utilize many different kinds of devices, some mechanism may help reduce the risk of attacks in some devices; while for others it could be inappropriate. For instance, IDS developed for personal computers can be used to secure the incoming/outgoing traffic from/to a proxy machine; whereas, in some devices, such as the power grid sensors and meters, IDS could be embedded into the devices themselves, which may result in the limitation of the features or abilities of the IDS.

Because many smart grid devices such as meters and sensors are embedded systems, energy usage and resource constraints of those devices could introduce another issue. For example, due to the limitation of memory size, embedded systems may not be able to include large signature libraries so it is possible that malicious software like a virus may successfully infiltrate the system without detection. Also, false positives could occur when detecting the actions tampered by either natural incidents or adversaries. Furthermore, tamper-resistant/tamper-evidence mechanisms are required to be cost effective and mass producible, since a large number of devices will be deployed in the Smart Grid. Hence, both tamper resistant and evidence must be designed or architected in such a way that they provide security, scalability, secure software and firmware updates, resistance to false positives as well as cost-effective mechanisms.

The research in this area is to provide scalable and cost-effective techniques to improve tamper-resistant mechanisms and make them difficult and/or more time-consuming for an attacker to break into the systems. Also, it should provide specific ways to prove that the protected object has been tampered with and/or to indicate who might have tampered with it. More importantly, because no single solution can be applied to the entire smart grid system, the research should provide a specific technique to a specific element of the Smart Grid.

4.2.2 Patches and Updates

Millions of devices, such as IEDs, Smart Meters, etc. will be eventually deployed in the Smart Grid system. There will be some scenarios where software and firmware need to be updated,

such as security fixes or software upgrades. The devices must be able to authenticate that the patch that they are downloading comes from a legitimate source; otherwise, any adversary may make use of malware or malicious software to break into the system. Moreover, the mechanisms for software and firmware upgrades will be different in different parts of the smart grid. For instance software upgrades for personal computers or computer gateways may require user consent before updating. Thus, users by themselves can verify that the patches or updates are coming from the intended source. However, in the case of firmware updates on devices such as IEDs, Meters, PLCs, etc., upgrading them cannot be the same as upgrading software. Since millions of devices are deployed in many places and environments, these upgrades must be autonomously performed. Also, there must be mechanisms to authenticate and ensure that the upgrades that will be set into the devices have not been modified at any time. Furthermore, it is possible that after the update has been installed into devices or computers, unexpected consequences could take place to reduce availability constraints. Thus, the maintenance processes and software testing must be considered in the first place.

The research in this area aims to provide a secure patch and update management processes in order to prevent the system from facing the issues specified above.

4.2.3 Information Handling Practices

Information is sometimes sent to utilities, third party contractors or other entities. The information, such as customers'energy usage and meter information could be shared among those relevant entities. Contractors may perform some kinds of collection of private data. Reusing and disclosing personal data by either utilities or third party could affect the privacy of customer information. Therefore, the information must be controlled in a secure manner such that only the necessary information of the customer is provided to any data collection entity and only authorized entities can access and use customer information. Also, the utility must obtain individual's permission prior to using personal information or disclosing private data to a third party. The amount of time that a utility may retain customers' energy usage information must also be specified. There are privacy issues that have to be considered in this area of research as well.

Privacy within Smart Grid is composed of the four dimensions as follows:[152]

1. **Privacy of personal information**

   Personal information is the information related to an individual in some specific aspects, such as names, photographs, SSN, etc. The privacy of personal information is sometimes called information/data privacy. It involves the right to control and use of data, of individuals with respect to when, where, how, to whom, and to what extent the information can be shared with and used by others, as well as to guard when the information is disposed

[152] A. Lee, T. Brewer; The Cyber Security Coordination Task Group, "DRAFT NISTIR 7628 - Smart Grid Cyber Security Strategy and Requirements", September 2009 [online]. Available: http://csrc.nist.gov/publications/drafts/nistir-7628/draft-nistir-7628.pdf

appropriately. This dimension is of the most concerns in the areas of Information Technology.

2. **Privacy of the person**

   This is concerned with the right of individuals to control the integrity of an individual's body. Medical treatments and procedures, such as providing blood and tissue sample, and biometric measurements are some of the examples of this dimension.

3. **Privacy of personal behavior**

   This involves the right of individuals to desire freely on their own decisions regarding their activities, such as political activities, sexual preferences, religious practices, etc. It also involves the right to keep certain personal behaviors from being shared with others.

4. **Privacy of personal communications**

   This is the right of individuals to desire the freedom to communicate with others, using various media, without being recorded, monitored or censored.

The information retained in the smart grid systems should be categorized into those four dimensions and must be considered as it can result in the invasion of privacy, if it is not securely protected. Research is needed to determine what types of information in the Smart Grid could create the privacy risks, and to specify the privacy impacts for those four dimensions.

Research in this area should not only to identify how information in the smart grid systems can be stored and managed, but also to identify and describe privacy concerns and impacts within the Smart Grid. The research on the privacy concerns should include, but not limit the following: [153]

- Exploring how the existing information in the Smart Grid could lead to privacy risks
- Identifying potential privacy problems and impacts
- Providing policies and practices in order to protect privacy and avoid misuse of personal information used within the Smart Grid

4.2.4 Physical Security

Physical attacks on the devices, such as meters and IEDs could make an attacker gain a cryptographic key and other secret information embedded in the devices because, the key material could be embedded in the device. This may lead to key handling and storage problems, since if the device is stolen or disposed, the knowledge of the secret information retained in the device might be leaked. One possible solution to this is to separate critical information, such as the crypto key into multiple independent parts, so that there must not be

---

[153] M. Enstrom, "(DRAFT) Privacy Chapter Introduction", April 06, 2010 [online]. Available:

http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/NISTIR7628PrivacyIntroApr2010

any single entity possessing enough information by itself to reconstruct the secret. For example, random numbers could be placed into a device along with an out-of-band communication channel. The out-of-band channel could be an activation code or serial number which the user could only obtain confidentially in order to activate the device. To activate a meter, for instance, the maintenance personnel may obtain the activation code by calling the provider. Moreover, if the device has been stolen or removed from the system after the installation, it needs to be re-activated before it can be re-installed into the system in order to ensure that the stolen device is not successfully used by an attacker. The research is to provide the appropriate mechanisms that can handle the issues specified above.

4.2.5 Role-Based Access Control (RBAC)

As discussed in the section 3.1.4, Discretionary Access Control (DAC) policy could be implemented in some part of the smart grid systems, but it has major issues that the policies may not be controlled by a central authority since the owner of the object can change or give the access rights to others. Also, there is a need for extra security mechanisms to prevent unauthorized copying when an access rule is given by the owner. On the other hand, Mandatory Access Control (MAC) may be more appropriate for multi-level secure military organizations. Role-based Access Control (RBAC) could be one of the effective means to control the accesses to the system in more central and secure manner, especially in an enterprise system like the Smart Grid. In RBAC the access decisions are made by roles or responsibilities that the users or subjects have in the organization. Access rights are categorized by role name and the attempt to perform an operation that is not associated with the given role will be denied. Thus, it can encapsulate the job functions one needs into one role. The modification to that role can be made without affecting other roles. This makes it easier for an administrator or security authority to control and manage the access policies.

However, the complexity when implementing RBAC in the smart grid systems is that role engineer becomes very difficult since the Smart Grid will contain a large number of entities, including users and devices, of which the responsibilities are various. For example, auditors should have the ability to read and verify states of the devices including remote attestation, but must not be able to configure the devices. Administrators can add, modify and remove users and their access rights in the systems and so on. Defining roles of all the entities in the system would become very difficult since some operations may be generally performed by most of the users and users belonging to different roles may have some common operations. It is rare to have all the operations needed to perform a job function can be neatly encapsulated into the same role definition without duplicating with other definitions.

One of the challenges of implementing RBAC is to find the balance between stronger security and easier administration. Most likely, the higher security is, the more granular the roles become. Hence, one user may be assigned to multiple roles. In this kind of situation, the administration tasks become more complex and inefficient. To deal with this issue, role hierarchy could be implemented. A role hierarchy is used to simplify role definitions by combining roles. In other word, one role may contain other roles. For example, the role called “Security Manager” may contain the roles of “Auditor” and “Security Officer”. Thus, an

administrator does not need to repeatedly list all the operations that are required for the Security Manager role. Role hierarchies are usually complied with the structure of the organization. The uses of role hierarchies help reduce the complexity of the administration tasks and simplify the number of roles assigned to the entities.

Another challenge is to define the policy in order to preserve the principle of Least Privilege -- a subject or entity in the system must be given the privileges that are necessary for its task, but no more. It is often that operations grouped into a particular role may be unnecessary for that role because of a variety of attributes and constraints of the job function. To describe access rules and policies, this principle must be considered. Thus, identifying what appropriate roles for the participants are and what functions should be performed on different Smart Grid environments by those roles is very crucial.

Research in this area should help specify clearly what types of roles users (e.g. Auditors, protection engineers, security officers, etc.) partake in the system and what operations should be permitted for the roles specified on various components of the smart grid systems. Additionally support for both hierarchical and non-hierarchical roles, emergency bypass of normal role assignment will be needed in keeping with high priority goal of availability.

4.2.6 Trust Management

Many kinds of elements, such as utilities, consumers and communication networks either local or long-distance transmission, involve Smart Grid systems. Trust management plays the role of determining how an element becomes trustworthy or reliable to others elements, and also in specifying and enforcing security policies to the system. Since the elements could be people, processes or technologies and could perform different operations, identifying who or what should be trusted and to what level is very crucial in Smart Grid systems. For instance, private networks should be more trusted than public ones. Moreover, access and identity management should be implemented in such a way that only authorized elements can perform certain functions based on their responsibilities. The main issues in trust management are how authorization and authentication between different entities can be implemented. The area of trust management is very broad and requires further research since eventually there will be the integration of different domains, from meters to demand response control centers or from SCADA systems to AMI systems. R&D issues in this area follow.

4.2.6.1 Trust Modeling

Trust Modeling is a process of how to define threat profiles and mechanisms that respond to those profiles.[154] Since there will be a number of elements involved in the system, it is essential to determine how trust can be established and how the degrees of trust can be assigned to an individual or process. It is important to determine what security issues could take place when different domains communicate with each other, and what the impact level and actions

---

[154] D. Andert, R. Wakefield, and J. Weise, Professional Service Security; Sun Microsystems Inc., "Trust Modeling for Security Architecture Development", December 2002 [online]. Available: http://www.sun.com/blueprints/1202/817-0775.pdf

corresponding to those issues would be. The major purpose of the trust model is to provide the framework for enforcing security mechanisms of how to respond to those issues.

The research in this area is to develop and refine trust models that could be used as a representative environment to assess the impacts of the security issues across the domains, such as unauthorized accesses, Denial of Service (DoS) attacks, and misconfigurations, as well as to indentify strategies to respond to those issues. Also, a trust model must provide the means to authenticate an entity's identity for specific events or transactions. The result of the research should provide a clear view of how to determine specific threats, vulnerabilities, and risks of the specific domain and also the response to those specific threat profiles.

4.2.6.2 Trust Management System

A trust management system provides a standard approach to specify application security policies, and credentials[155]. One of the common trust management systems that could be implemented in the smart grid systems in order to specify and enforce security policies and access control is KeyNote. KeyNote is designed to work well with a variety of sizes of applications, including large-scale and Internet-based applications. KeyNote provides a standardized language for specifying security policies, trust relationships and digitally-signed credentials that are used to control accesses and requests across untrusted networks. KeyNote could be useful in the smart grid because the security policies are written in a standard language meaning that across the different applications on different domains, the language for expressing and enforcing security policies still remain the same and it is defined outside the application code which makes it easy to alter the policies whenever needed. This chapter is intended to provide an overview of KeyNote. The further detail of KeyNote which is publicly released is described in RFC 2704[156].

The research in this area is to take into account the nature of smart grid systems, which is distributed across different domains, on how security policies and credentials can be specified using KeyNote. The outcome of the research should provide the standard security policies, which can be operated on a distributed basis, using a state-of-art trust management system, such as KeyNote.

---

[155] M. Blaze, J. Feigenbaum, and J. Ioannidis; AT&T Labs – Research, A. Keromytis; U. of Pennsylvania, "The KeyNote Trust-Management System Version 2", September 1999 [online]. Available: http://www.cs.columbia.edu/~angelos/Papers/rfc2704.txt

[156] M. Blaze, J. Feigenbaum, and J. Ioannidis; AT&T Labs – Research, A. Keromytis; U. of Pennsylvania, "The KeyNote Trust-Management System Version 2", September 1999 [online]. Available: http://www.cs.columbia.edu/~angelos/Papers/rfc2704.txt

4.2.6.3 Cross-Domain Security[157]

Smart Grid consists of power systems domain, IT domain, and if PEVs become an integral part of the grid, transportation domain. The study and research in what adverse activities could be performed in the cyber domain which affect the power domain are not very clear. The need to determine and detect security concerns and impacts from those concerns, such as intrusions, unauthorized accesses, misconfigurations, and to form a correct and systematic response to those concerns, as well as to ensure security without degrading the systems is important. The R&D in this area is to develop models and technologies in order to enhance the reliability of the power system, while ensuring the security in the cyber domain. Also, once the development and implementation of Smart Grid systems become pervasive, a further research into new security risks will be needed. Thus, further research for new security models and technologies will be eventually required.

Examples of research and development in this area are as follows:

- A Large-scaled and reliable security-event detection model that can be used in a cross-correlated manner and can operate on the smart grid without human interference. The model should be scalable enough to be operated on a distributed basis.
- Intrusion detection/prevention system or other technologies using models/methods specified above are necessary. The system should also provide the appropriate strategies to security events on a real-time or near real-time basis. This will help with incident response and forensic capability

4.2.7 Categorizing into Confidential and Non-Confidential

Most of the topics specified in this chapter can be researched in public domain. One exception the researchers feel should be confidential is cross-domain security, especially if this work is done on the model of a real system. In this case the results of the research should be confidential. The reason is because the results can inadvertently reveal vulnerabilities in a real smart grid system which attackers will most likely exploit. The researchers recommend that the research be conducted by assert owners in a laboratory setting, a national lab, or a University. In all cases those conducting the research, or those who see the results should sign non-disclosure agreement (NDA).

---

[157] I. Ghansah; California State University Sacramento, D. Thanos; GE Digital Energy, P. Pal, and R. Schantz; BBN, C. Gunter, T. Yardley, and Himanshu Khurana; University of Illinois, E. Beroset; Elster, S. Klein; OSECS, R. Jepson; Lockheed Martin, J. Ascough, and R. Henning; Harris Corp. P. Blomgren; SafeNet, G. Emelko; ACLARA Tech, K Garrard; Aunigma Network Security Corp, "R&D Themes for Cyber Security in the Smart Grid", March 25, 2010 [online]. Available: http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CSCTGRandD/RDIdeas-March30_2010.doc

4.3 Potential Research Topics in Cryptography and Key Management

4.3.1 Public Key Infrastructure (PKI)

Asymmetric or public key cryptography can be used to implement security goals, such as confidentiality, integrity and non-repudiation. However, to successfully provide these goals, there is the need to ensure that a given public key is from the alleged source and can be trusted. Since the public key is usually made available to the public, it could be published by an adversary as well as the legitimate user. This trust issue has led to the use of Public Key Infrastructure (PKI) and public key certificates. This section is intended to give an overview of PKI related to the issues specified in section 4.3.1.1, 4.3.1.2 and 4.3.1.3.

PKI is a system that is widely used for the establishment and distribution of digital certificates that bind a user's' identity and its public key together in order to ensure that the specific public key belongs to the specific identity. The main purposes of PKI are to manage public keys and enable the uses of public key cryptography and digital certificates through the use of Certificate Authorities (CAs) and Registration Authorities (RAs) in insecure environment, such as Internet. Two major components of PKI are as follows:

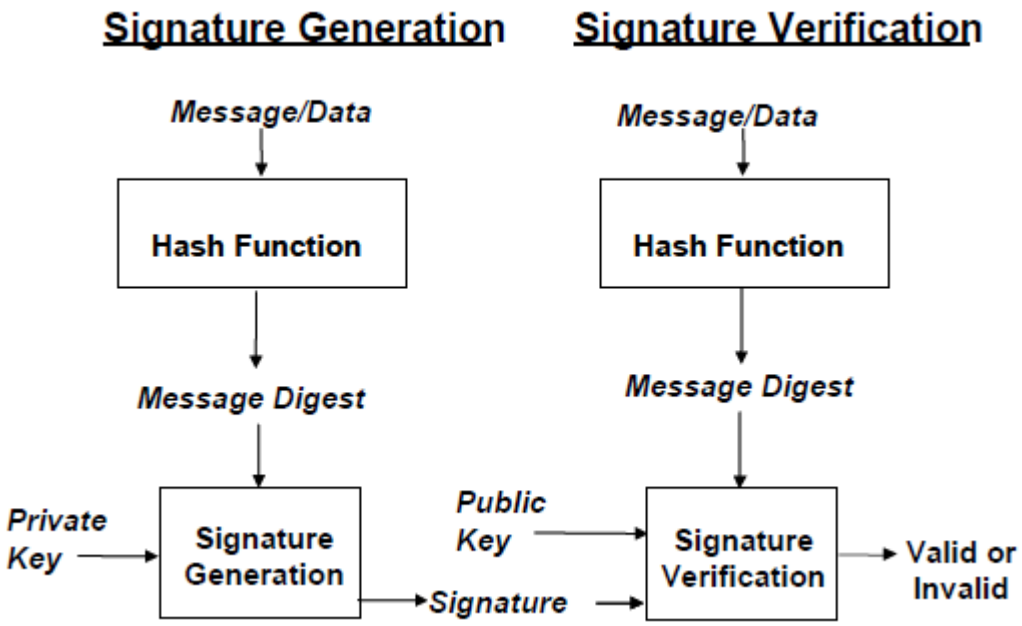
- Certificate Authority (CA)
- A CA is "an authority trusted by one or more users to create and assign public key certificates."[158] The CA is sometimes called a trusted third party which is responsible for providing various key management services and publishing a public key bound to a given user. This is done by having the CA create a message containing the entity's public key and identity and digitally signing the message with its private key. This message is called a digital certificate. The detail of digital signature is described in the next section. CA can be an internal or external organization or a trusted third party who can certify the public key associated with the name and identity of the owner.
- Registration Authority (RA)
- In general, RA is an optional component that is used to perform administrative tasks which CA normally performs. A RA is responsible for verifying an entity's certificate request and determining whether an entity is qualified to have a certificate or not.

Overview of Digital Certificate

Digital certificates simply utilize the concept of a digital signature. Figure 4-1 shows the process of signature generation and verification.

[158] A. Arsenault; Diversinet, S. Turner; IECA, PKIX Working Group, "Internet X.509 Public Key Infrastructure: Roadmap", July 2002 [online]. Available: http://tools.ietf.org/html/draft-ietf-pkix-roadmap-09

Figure 4-1: Signature Generation and Verification159



Digital Signature is analogous to a hand-written signature. However, it is very difficult for it to be counterfeited because it can combine the name and identity of the signer. The signature part is generated by using a secure hash function, such as a message digest algorithm, and the sender's private key. The sender encrypts the hash of the original message using his private key. When the message is received, the recipient verifies that the message has not been altered in transit using the public key of the sender and the same hash function. The source of the message is authenticated, because only the corresponding public key can verify the signature. Thus, digital signature can provide both source and data integrity.

Typically, a digital certificate contains a public key, certificate information regarding the public key and digital signature of the CA. The certificate information can be the name and identity of the public key or subject data, the algorithm used and date range which is used to verify if the certificate is valid. The signature part of the certificate is derived from a public key and the credential of the public key owner; it is digitally signed with the CA's private key. The recipient of the certificate uses CA's public key to verity the certificate. Thus, the use of a certificate ensures that the public key in the certificate belongs to the owner or subject of the certificate.

Thus the use of PKI allows for the implementation of digital certificates which are used for ensuring that the public key is certified and comes from the source that it claims. After the public key is considered as the trusted, public key encryption, digital signature techniques, and so on, can be performed.

---

[159] National Institute of Standard and Technology (NIST), "Digital Signature Standard (FIPS 186-3)", June 2009 [online]. Available: http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf.

However, implementing PKI is not an easy task. Careful planning and proper design are critical. Thus, there are some research areas, which have to be explored before implementing a PKI, as follows:[160]

1. Trust Establishment
2. Private Key Protection
3. Certificate Revocation List (CRL) Availability

4.3.1.1 Trust Establishment

PKI largely relies on trust. To fully utilize PKI, the CA and RA must be trusted and must verify that the identity of the entity requests for a digital certificate is trustworthy. The requesters must be authenticated that they are what they claim to be. The issue is that appropriate and strong verification process must be provided, since CA and RA could be external and internal and could be individually implemented depending on the organization. In addition to the trustworthy verification procedure, the issue of trusting the actual CA needs to be considered as well as the security policy of the CA to ensure that the CA has an appropriate infrastructure and trusted personnel. Even though for years, vendors with infrastructure services have been providing certificate services, there is an issue regarding the cost of the certificates. Also, the ways to utilize certificates from those vendors may not be appropriate when applying those methods to some devices in the smart gird systems since there may be some resource constraints of the devices. Another issue is how to handle in the case where the user's private key has been stolen or lost with or without the notice of the holder of the key and he or she has reported it in order for the certificate to be revoked. A common method in this case is to place the key on a CRL. There are research issues regarding using CRLs for meters which needs to be addressed. There are more details on this in later sections.

4.3.1.2 Private Key Protection

Compromise of a private key will lead to the breaches in security goals, such as loss of confidentiality, integrity, and non-repudiation, since an adversary can use the private key to decrypt the message or digitally sign the message while pretending to be the actual owner of the key. Not only do the private keys of the users of PKI need to be protected, but the private keys of CAs need to be protected as well. Compromising the CA's private key would allow an attacker to create numerous illegitimate digital certificates and use those certificates for the malicious purposes. Thus, there must be a mechanism to investigate or detect that the private key has been compromised as quickly as possible; otherwise, vast amounts of adverse consequences could take place. To minimize the risk, generally, both the owners of the key, which could be a variety of devices, such as meters and personal computers, or persons, and the authorized issues of the keys must be protected using defensive measures such as Intrusion Detection System (IDS), Antivirus software, etc. Also, secure storage devices must be utilized.

---

[160] E.Stavrou, "PKI: Looking at the Risks", January 2005 [online]. Available: http://www.devshed.com/c/a/Security/PKI-Looking-at-the-Risks/

Nonetheless, since in the smart gird systems, a wide variety of devices and machines will be utilized, different technologies or means to store the secret information may have to be considered. More importantly, since those devices would operate with nearly no human interference, there should be the mechanism of how to report to the CA that a device or the key has been tampered with. Thus, there are a number of research issues that should be considered in this area.

4.3.1.3 Certificate Revocation List (CRL) Availability

Every so often certificates can no longer be considered trustworthy for various reasons including expired certificates, lost or compromised private keys, and the loss of devices that contain certificate information. A CRL is a list containing the serial numbers and revocation dates of all the digital certificates that have been revoked and no longer valid, and maintained by an issuing authority. The CRL is typically available to the public, so that any recipients of a signed message can verify that the certificate received has not been revoked and it is still valid. The issue is that CRL is the only way the CA can invalidate the certificates. Thus, CRL needs to be updated in timely manner. Also, it needs online validation, which may consume bandwidth of the networks. As a result, an adversary may try to attack the availability of the CRL, such as using Denial of Service (DoS) attacks, if the CRL is not available, no operation that depends on the acceptance of the CRL will be carried out. Also, there is the risk that the CRL becomes unavailable due to the machine containing the CRL is infected or compromised, for example; an attacker may be able to use an invalid certificate to trick others for malicious purposes. To minimize the risks associated with the CRL availability, the issuing authority must maintain secure architectures and strong defense mechanisms in order to avoid those security violations and fail-over plans in order to provide secondary architecture whenever the primary one has failed. Thus, there is a need for a research in this area so as to provide solutions to those issues specified above.

4.3.2 Key Management and Public Key Infrastructure (PKI)

There may be some situations in the Smart Grid where PKI is not appropriate since some devices such as smart meters would not be able to connect to key servers and Certificate Authority (CA). Smart Grid devices may contain both short-term symmetric and long-term asymmetric keys. Also, the smart grid systems will eventually involve millions of devices. Hence, key distribution is one of the potential issues in Smart Grid. The resource limitations of devices also pose some problems with respect to the size of keys and certificates. For example, if the size of certificate is too large, the validation process may be slow and battery life of the device may be shorter than expected. Moreover, the key should be re-negotiated from time to time in order to protect itself and reduce the risk of key being broken. To implement security mechanisms, appropriate key lengths and algorithms should conform to the recommendations from NIST, FIPS, RSA laboratories and other standards. For example, NIST SP800-57 (Part 1)[161]

[161] E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid; National Institution of Standard and Technologies (NIST), "Recommendation for Key Management – Part 1: General (revised)", March 08,

recommends using minimum 2048-bit key for RSA algorithm to protect data beyond 2010. In the case of symmetric algorithms, NIST SP800-57 (Part 1)[162] recommends using at least three keys for triple DES or at least 128-bit key for AES algorithm. However, legacy devices or systems could be used in the Smart Grid systems and may use smaller key size which the designer should include some extra mechanisms, such as time stamping and other techniques, to provide reasonable security level instead of depending on only cryptographic schemes used.

The research in this area is to provide best practices for key management in the Smart Grid, in which key sizes, key lifecycles for each key type and cipher used must be specified. Also, mechanisms to handle the security issues of resource limitations in legacy devices should be specified as well as the methods to deal with key distribution and certificate management in different kinds of environment, where PKI could be applied in the Smart Grid. There are more Key management issues. In cases where symmetric shared keys are used there is a different key management problem from public key systems. The problems are: Will the key be installed in devices at the factory? Will keys be installed by users? What if the keys are changed or need to be changed due to loss, theft, etc.

4.3.3 Alternative Ways of Obtaining Public Keys

To be able to utilize public key cryptography for encryption and digital signature in a trustworthy manner, certified public keys are needed. This requires that the public key certificates must be available and be obtained prior to using them in order to perform those operations. Also, there are issues of using PKI specified in the section above. There is an interest in the approaches which enable the use of public key cryptography to be performed without satisfying the requirement of retrieving the certified public key in advance. This section gives an overview of two of the possible technologies which are Identity based encryption (IBE) and Trusted Platform Module (TPM). These approaches could be used as an extensions or alternatives to a conventional certificate-based PKI in the Smart Grid as well. Research is needed to determine which of these approaches are appropriate in which areas of the smart grid infrastructure.

4.3.3.1 Identity Based Encryption (IBE)

Identity-based encryption (IBE) is "a public-key encryption technology that allows a public key to be calculated from an identity and the corresponding private key to be calculated from the

---

2007 [online]. Available: http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf

[162] E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid; National Institution of Standard and Technologies (NIST), "Recommendation for Key Management – Part 1: General (revised)", March 08, 2007 [online]. Available: http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf

public key[163]."IBE enables senders to encrypt messages for the recipient without requiring a recipient's public key to be established, certified, and published[164]. Thus, the complexity of the encryption process for both users and administrators are greatly reduced. The advantage is that the sender does not need to hold the recipient's public key prior to sending the message, as it can be calculated by the sender. This is different from common public key technologies used in today's Internet communications which need exchange of keys prior to the start of encrypted communication. The ability to calculate a recipient's public key, in particular, eliminates the need for the sender and receiver in an IBE-based messaging system to interact with each other, either directly or through a proxy such as a directory server, before sending secure messages.

The Figure 4-2 describes the operations of encryption/decryption of an IBE system. The two main components in the IBE are as follows:

- Private-key Generator (PKG)
- A PKG contains a master secret which is used for generating an individual's IBE private key. An individual needs to send a request for the IBE private key to the PKG and be authenticated before obtaining the IBE private key.
- Public Parameter Server (PPS)
- A PPS contains IBE public parameters and policy information, such as IBE algorithm and key strength, for an associated PKG. The sender of the message must obtain the IBE public parameter that is used for calculating the recipient's public key from the PPS. The IBE public parameter contains all the information that is necessary for the creation of the encrypted message, except the identity of the recipient. The PPS can also provide the URI (Uniform Resource Identifier) of the PKG where the recipient of an IBE-encrypted message can obtain the IBE private keys. Because the uses of public parameters are very crucial in the IBE, thus the public parameters must be transmitted via a secure communication protocol, such as TLS.

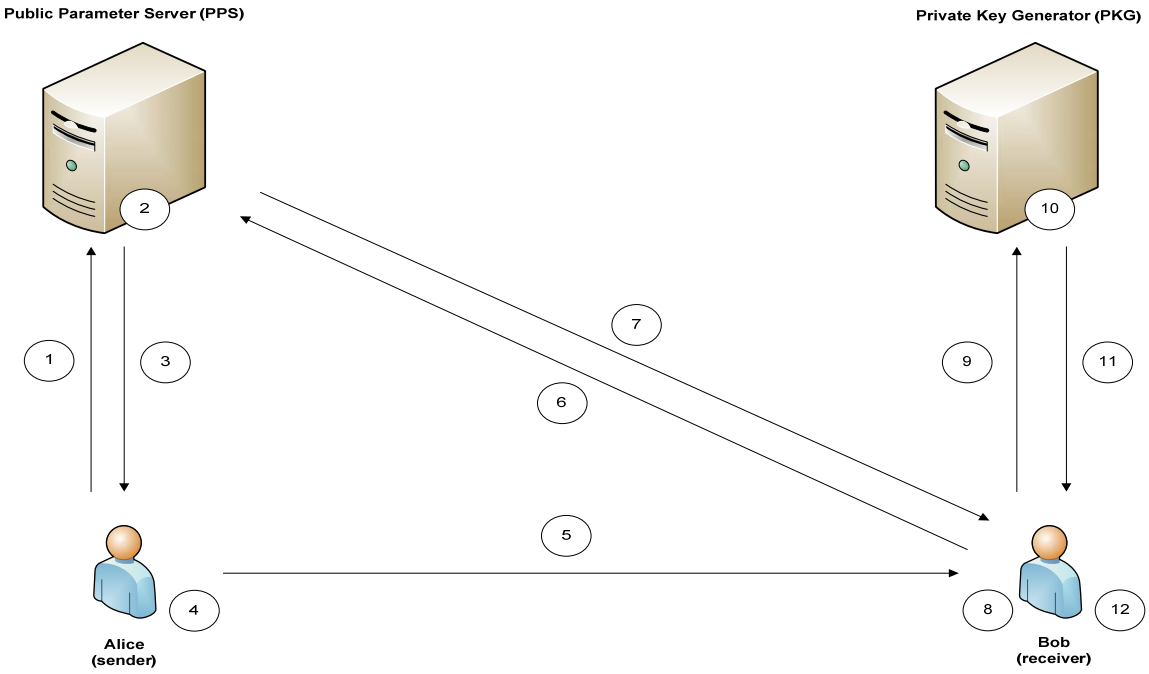
The sender of an IBE-encrypted message chooses the PPS and corresponding PKG according to his security policy. Different PPSs may provide different public parameters, such as different IBE algorithms, different key strengths, or different levels of authentication before granting IBE private keys.

---

[163] G. Appenzeller, L. Martin; Voltage Security, M. Schertler; Tumbleweed Communications, "Identity-based Encryption Architecture", Internet Draft, November 2007 [online]. Available: http://tools.ietf.org/html/draft-ietf-smime-ibearch-06

[164] M. Gagné, "Identity-Based Encryption: a Survey", RSA Laboratories Cryptobytes, Vol. 6, No. 1, Spring 2003

Figure 4-2: Operations of Identity Based Encryption[165]



The steps in figure 4-2 are categorized into the steps of sending IBE encrypted messages and receiving IBE encrypted messages which are described as follows:

Sending IBE encrypted messages

1. Alice sends the request for IBE public parameters to the PPS.
2. The PPS authenticates the request.
3. If step 2 is successful, the PPS sends the IBE public parameters to Alice. Then, Alice calculates the Bob's public key by using the public parameters and Bob's identity.
4. Alice constructs the encrypted message by choosing a content-encryption key (CEK) and encrypt the data, which she wishes to send to Bob, with that CEK key. Then, Alice uses Bob's public key to encrypt the CEK. Thus, the encrypted message will at least be the combination of the encrypted data and encrypted CEK.
5. Alice sends the encrypted message to Bob.

[165] A White Paper by Vertoda, "An Overview of Identity Based Encryption", 2009 [online]. Available: http://www.slideshare.net/vertoda/an-overview-of-identity-based-encryption

Receiving IBE encrypted messages

1. Before Bob can decrypt the message, he needs at least two components, the same public parameters as Alice and the necessary private key. Thus, Bob needs to send the request to the PPS in order to obtain the public parameters that were used in the encryption process.
2. If the authentication process is successful, then the PPS sends the IBE public parameters to Bob.
3. Bob calculate his own public key by using the public parameters received from the previous step.
4. Bob provides the public key, his authentication credentials and the private key request to the PKG.
5. The PKG authenticate the request from Bob.
6. If step 10 is successful, Bob will obtain the private key from the PKG.
7. Bob uses the private key received to decrypt the CEK part of the encrypted message. Then, he uses the CEK to decrypt the encrypted data part of the message.

The concern with IBE is that it requires a centralized server. This means that some keys have to be generated and stored which exposes a threat. The authentication mechanisms used by the PPS and PKG are needed for verifying the requests from both senders and receivers of the messages. Also, it requires secure a channel between a sender or recipient and the IBE servers for transmitting the recipient's private keys and IBE public parameters. Moreover, there may be some issue regarding how the recipient store the private key received from the PKG. Finally, IBE only provides encryption and hence digital signatures must be provided separately. The further details of how to implement IBE can be found in RFC 5408[166].

4.3.3.2 Trusted Platform Module (TPM)

Trusted platform module is both the name of published specification detailing a secure crypto-processor that can be used to store cryptographic keys as well as the general name of the implementations of that specification[167]. The implementation of TPM is basically a secure micro-controller with cryptographic operations, such as secure the generation of cryptographic keys, hardware pseudo-random number generator, etc.

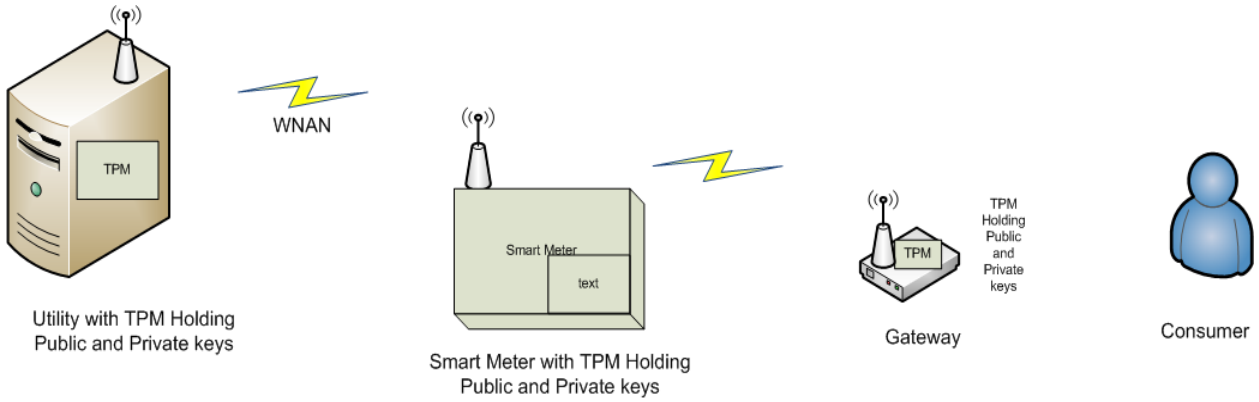
Figure 4-3 describes where the TPM could be installed in all the critical end points in the smart grid systems (i.e. Gateway, Smart Meter, Utility head end).

---

[166] G. Appenzeller; Stanford University, L. Martin; Voltage Security, M. Schertler; Axway, "Identity-based Encryption Architecture and Supporting Data Structure", January 2009 [online]. Available: http://tools.ietf.org/search/rfc5408

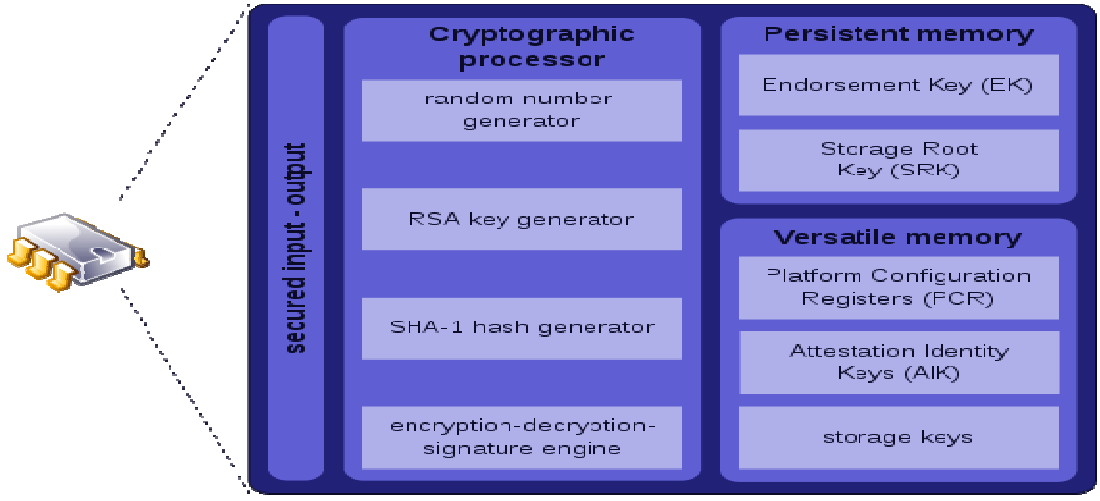
[167] WikiPedia, "Trused Platform Module", April 2010 [online]. Available: http://en.wikipedia.org/wiki/Trusted_Platform_Module

Figure 4-3: Use of TPM in the HAN Environment



In general, putting security services into the hardware and using those in conjunction with software solutions provide higher security level than those that use only software to provide security.

Figure 4-4: Internal Components of TPM168



The TPM provides a set of cryptographic capabilities, such as RSA key generator, random number generator and so on, that allow cryptographic functions to be executed with in the TPM hardware[169]. Hardware and software outside the TPM do not have permission to access and execute these cryptographic functions. TPM contains a hardware engine that is used to perform RSA encryption/decryption by using the Endorsement Key (EK), which is a 2048-bit RSA

---

[168] WikiPedia, "Trusted Platform Module", April 2010 [online]. Available: http://en.wikipedia.org/wiki/Trusted_Platform_Module

[169] S. Bajikar; Mobile Platform Group, Intel Corporation, "Trusted Platform Module (TPM) based Security on Notebook PCs – White Paper", June 20, 2002 [online]. Available: http://www.intel.com/design/mobile/platform/downloads/Trusted_Platform_Module_White_Paper.pdf

public/private key pair. The EK is unique and randomly created by the manufacturer and cannot be modified. The private key generated with the TPM never exposes outside the TPM.

Before a TPM machine can be used, the identity of the machine needs to be authenticated with the verifier. Since each TPM has a unique RSA key embedded in the chip at the manufactured time, this key could be used for authentication as well. For example, it can be used to verify that a system that is trying to gain access to is the intended one. However, the use of the EK to authenticate the identity of the TPM may prose privacy concerns to the user, since the EK uniquely identifies the machine. Thus, Attestation Identity Key (AIK) is developed for solving this privacy issues.

The AIK is a key generated for use in attestation. AIK is bound to the TPM's identity, which is in turn tied to the TPM's EK. Whenever, a TPM needs to be authenticated, an AIK will be generated as a second RSA key pair. The public key part of the AIK will be sent to a privacy CA, a trusted third party, to authenticate this public key with respect to the unique EK. If the CA can verify that the EK of that TPM is in its list, it will issue a certificate on that AIK. Thus, the TPM can then use this certificate to authenticate itself with the verifier. Nevertheless, this approach still has the issue that the privacy CA has to be highly available, since, in every transaction, the CA needs to be involved. Also, privacy concerns are rise, if the privacy CA and the verifier collude. For example, if somehow the transaction records of the privacy CA are revealed to the verifier, the verifier may be able to uniquely identify the TPM, since the AIK is still tied to the EK.

There is an ongoing research to try to find out the solutions to the issues discussed above. One of the solutions is called, Direct Anonymous Attestation (DAA), which enables remote authentication while preserving the user's privacy. DAA has been included in the latest TPM specification[170] by Trusted Computing Group (TCP) and is still under development. Thus, there is a need for research in this area on how to deal with the CA availability and privacy concerns in TPM.

The research in this area is to provide the solutions to the issues of the retrieval of the keys and certificates. The two proposed approaches discussed in this section could be one of the solutions. However, given that each of the approaches has their own advantages and disadvantages and since additional techniques would be utilized in order to solve the issues addressed, such as providing digital signature in the IBE or the authentication mechanisms used by the PPS and PGK, there is a need for research to address and find the solutions to those issues.

4.3.4 Limitation in Devices and Cryptography

Smart Grid will be utilizing various kinds of hardware devices, such as sensors, meters, IEDs etc. Those devices may have some resource limitations, such as battery life, bandwidth, CPU

[170] TPM specification, version 1.2, Revision 103.
http://www.trustedcomputinggroup.org/resources/tpm_main_specification

and memory. For example, in sensor network, Elliptic-Curve Cryptography (ECC) could be an attractive approach for providing security in Wireless Sensor Networks (WSN), since it utilizes smaller key size and less energy than the cryptographic schemes used in the Internet communications, while providing equivalent security level as other algorithms. However, there is still ongoing research on how much memory a sensor will need in order to keep the secret information, such as keys and certificates, and also how much energy a sensor will consume for the computation of encryption and decryption using different key sizes. Also, resource limitations introduce new kinds of attack which tries to drain battery life and memory resources. Thus, it is necessary to address those limitations and choose the appropriate mechanism in order to ensure security goals as well as overcome those limitations. The outcomes of the research in this area should provide the specific solutions or best practices to those issues addressed above on a specific device.

4.3.5 Categorizing into Confidential and Non-confidential

The researchers do not consider any of the R&D topics in this chapter to be confidential.

4.4 Specific Domain Topics

4.4.1 Choosing a Standard for Implementing NAN

There are quite a few technologies in contention to be used to implement neighborhood area network. The technologies under consideration in the implementation of neighborhood area network for Smart Grid are shown in table 4-1.

Table 4-1: Summary of Technologies under Consideration for Neighborhood Area Network[171]

Technology	Features	Advantages	Disadvantages
IEEE 802.11 (Wi-Fi)	Data Transfer Rate: 22 Mbps – 128 Mbps* Range: up to ½ mile Operating Frequency: 2.4 GHz to 5 GHz Applications: Meters (AMI), Distribution Automation (DA)	Low device cost Suitable to Mesh topology Low latency	Not yet proven for Smart Grid deployment
IEEE 802.16 (Wi-Max)	Data Transfer Rate: 30Mbps Range: up to 50 km Operating Frequency: 2 GHz to 3 GHz Applications: Meters(AMI), DA, Mobile workforce management	Low latency High bandwidth	High equipment or device cost Not yet proven for Smart Grid deployment
IEEE 802.15.4	Data Transfer Rate: 250 Kbps Range: 100+ meters Operating Frequency: 1 GHz to	Suitable for Mesh topology Low power	Lesser data rates Short range coverage

[171] J. Fox, B. Gohn, C. Wheelock, "Networking and Communications, Energy Management, Grid Automation, and Advanced Metering Infrastructure", PIKERESEARCH, 4Q 2009.

Technology	Features	Advantages	Disadvantages
	2.4 GHz Applications: Meters (AMI), HAN	consumption	
Cellular	Range: up to 50 km Operating Frequency: 900 MHz to 2.4 GHz Applications: Meters (AMI), DA, Mobile workforce management	Uses existing networks Low capital investment Short time-to-market Low module cost	No direct utility control over the network Moderate performance
RF Mesh	Data Transfer Rate: up to 1 Mbps Range: Variable Operating Frequency: variable Applications: Meters (AMI), DA	Customizable based on specific need Self-healing and organizing Low cost	Proprietary Expensive devices Unpredictable Latencies
Leased Lines (e.g. SONET)	Data Transfer Rate: 1.5 Mbps – 155 Mbps Range: Variable Operating Frequency: Wired (Fiber or copper cables) Applications: Substations, DA	High Performance Robust	High recurring cost No direct utility control Not available at all sites
Broadband over power lines	Data Transfer Rate: 256 Kbps – 10 Mbps Range: Variable Operating Frequency: 1.8 to 80 MHz (electric carrier) Applications: Substations, DA	Low recurring cost Robust	High initial investment Expensive devices Not widely implemented Not reliable
Narrowband over power lines	Data Transfer Rate: 1 Kbps – 100+ Kbps Range: Variable Operating Frequency: 9 KHz to 95 KHz Applications: Meters (AMI), DA	Widely deployed in Europe Proven and Robust	Low performance High latency

A preferred standard would be the one which is compatible or common across multiple domains like HAN, NAN and WAN. This would decrease the equipment cost to a great extent and also reduce the complexity of the implementation since the devices would only need to support only one technology standard. If not a single technology, lesser variations used across the domains, the better it is. To explain this in more detail let us consider an example.

The most obvious technology considered for HAN is ZigBee, which is based on IEEE 802.15.4. ZigBee derives the implementation of PHY layer and the MAC layer from the IEEE 802.15.4 standard. If IEEE 802.15.4 is considered for the implementation of NAN, the same radio could be used in the devices installed at homes and utilities. The same packet format could be maintained and so on. This would ease the implementation and lessen the equipment costs.

Also, it would be more advantageous if an existing technology is chosen, or modifying an existing technology to satisfy the Smart Grid NAN deployment requirements. Technologies, such as Narrowband over power lines, which are proven and robust in Europe, could be considered. The advantage of using such a technology is that no new deployments are required as it uses the existing power lines for data transmission, also data could be modulated using the AC 60Hz frequency as a carrier.

To date the researchers know of no proven or widely deployed technology in North America to be used for the implementation of neighborhood area network. Hence research is required in this area to choose a protocol based on the above discussion as well as security issues associated with the protocols.

4.4.2 Virtual Environment for Customer Domain Gateway

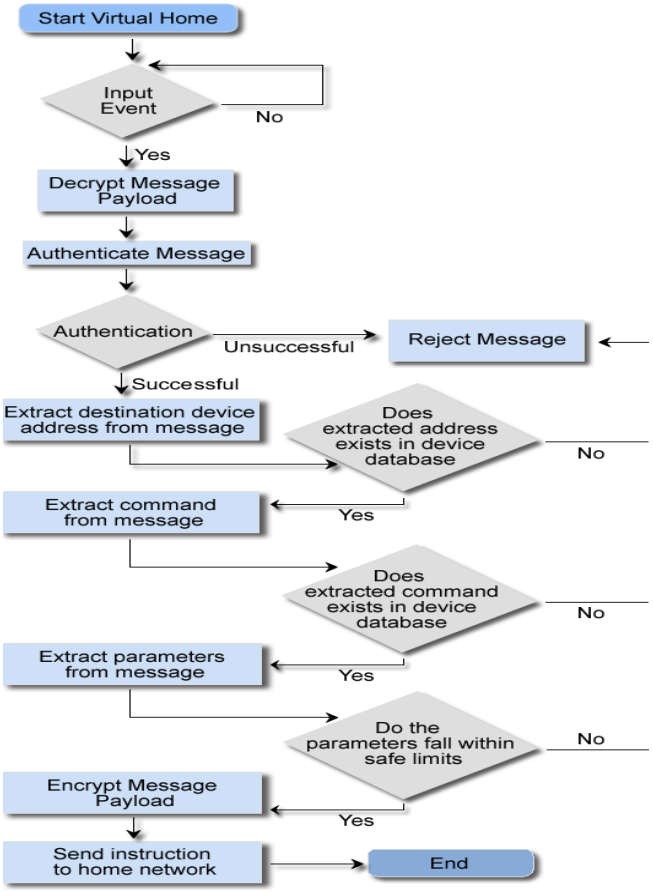
Since a gateway acts like a single point of entry for external entities to enter a home area network, it is being discussed as an ideal platform for virtualization. The virtual environment includes the entire home area and the sensitive data associated with the home area network. One such solution has been proposed by Khusvinder Gill, Shuang-Hua Yang, Fang Yao, and Xin Lu in A ZigBee-Based Home Automation System[172]. In this they suggest a virtual home which is software constructed in C programming language. The virtual home is implemented on the home gateway. All communication and instructions are checked, as illustrated in Figure 4-5, for security and safety in the virtual environment, before implementation in the real home environment. This is a very effective way to mitigate any intrusion into the real environment. Since this is such a vital contender for providing isolation from the threats, it is also a viable target for attackers, as data which comes from the virtual home is completed is trusted. If this is compromised then attackers can cause serious damage to the home environment. Virtualization can be extended not only to the home area network but can be used in the utility side as well.

There are areas in the virtualization field that need intense research, such as if the network is made scalable how the virtual environment would behave and if the protocols are varied what would be the effect. The entire virtual environment resides in an enclosure which is held in the remote location, which puts constrain on the power requirements. The encryption techniques that are used be low on power budget, whether the virtualization provided will be embedded solution or will it be a completely software based solution. To provide a virtual solution which is power efficient is an area that needs extensive research. The database in the virtual environment is in constant contact during the authentication process is a definitely area of concern, as in what kind of memory will be used to store the sensitive information is an area of research.

---

[172] K. Gill, S. Hua Yang, F. Yao, and X. Lu; IEEE Transactions on Consumer Electronics, "A ZigBee-Based Home Automation System", Vol. 55, No. 2, May 2009 [online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=05174403

Figure 4-5: Virtual Home Flow Chart



Virtual environment can be a very power and effective tool in the smart grid implementation provided it has been thoroughly researched for loop holes and flawless before deployment.

4.4.3 HAN Devices and HAN Gateways Authentication

A smart meter and other device could be used as a gateway in order to receive and demand response to DR signals from/to utilities and DR services providers. HAN devices will respond to the DR signals received according to DR strategies, which could be pre-programmed in the devices. However, it is possible for an attacker to forge a DR command and inject it into HAN. Also, an attacker may be able to join his own device to the network in order to intercept the traffic or perform malicious attacks. It is crucial that authentication mechanisms must be provided in such a way that when a device receives a command, it must be able to ensure that the command is come from the legitimate source and is delivered to the correct device. When the authentication fails, the device should not respond to the signal and/or should be able to report back to the DR head-end. Cryptographic schemes, such as digital signature or message authentication code, could be used to provide such a protection.

Research in this area is needed to provide specific methods for such authentication. However, it is necessary to consider the techniques that can be implemented in different kinds of devices

since HAN devices could be gas meters, water meters, lighting controls, in-home monitors, thermostat, etc. Each of the devices may have some limitations, such as resource limitations or inability to store data permanently, and only cryptographic tools may not be sufficient enough to ensure the authentication between those devices. Also, since to some extent, HAN devices could be obtained and installed by consumers, the authentication process should be operated on autonomous basis to simplify things for the consumer.

4.4.4 DR Services Providers and Smart Devices Authentication

DR signals and control commands could be sent directly from DR Service providers to smart appliances, HAN devices or Energy Management Control System (EMCS) this applies to situations where the signal sent without going through HAN gateways in order to control energy usage by shifting or shedding electrical loads at participant's sites or control the devices. However, an attacker could also send false signals or inject any malicious commands to those devices. If an attacker successfully injects false commands into the system, it could have a tremendous impact on the stability of the grid and energy consumers' billings. Authentication of DR signals sent between DR services providers and other smart appliances is crucial. The system must provide a mechanism to authenticate to ensure that the commands are sent from alleged sources to intended devices properly. If a command is sent in an unauthorized manner the command should be rejected and the devices must not respond to it. Also, the response from the devices should be sent to indicate that the commands received are successfully carried out. Cryptographic techniques, such as digital signature, could provide such a protection. However, devices such as meters, sensors, and other HAN devices, have resource constraints including limited memory, storage, and battery life as well as bandwidth. These limitations should be considered when utilizing mechanisms to provide authentication as well.

The research in this area is to provide specific solutions to those issues addressed above. However, there may be situations where the cryptography may not be utilized adequately, since there will be many different kinds of devices deployed in the smart grid system. The research should also identify these limitations and/or provide best practices or means to handle those issues as well.

4.4.5 Authentication and Authorization between Users and Smart Appliances and/or HAN-Based Monitors

User authentication is important in smart grid systems, since users could be maintenance personnel, IT personnel or home users. Thus the way to authenticate users should be friendly enough for home users who may not possess technical skills. Password authentication is one of the possible techniques that could be implemented. Currently many smart meters are using this technique to authenticate maintenance personnel. Also, since access to smart devices can be local or remote through AMI or HAN gateway, an attacker may attempt to gain access to the devices as well. Therefore, the system should provide mechanisms to defend the system from password attacks, such as dictionary and brute force attacks, and also limit the attempts to perform those attacks to the system.

Once a user is successfully authenticated and gains access to the system, authorization techniques must be applied. Authorization refers to the act of granting a user or device proper

rights to access some particular resource of the system. The issue is that different users could have different functions to perform on the devices. For example, a home user should not have permission to change or reset some important configuration values like energy price and monthly usage in the meter. To provide authorization, access control mechanisms are necessary. Access control mechanisms, such as Role-based Access Control (RBAC), must be described and utilized in order to ensure such that the users can only perform the tasks they are allowed. Details of RBAC are described further in this chapter.

Thus, authentication and authorization should be able to ensure that only authorized users can perform certain functions on specific devices.

The research in this area is to describe the potential issues of password attacks that could be manipulated by an adversary and provide defense mechanisms to those issues. Also, it should identify an appropriate set of roles and determine how these roles can perform particular tasks on particular devices. Finally, it should describe access control policies and provide the techniques to implement those policies in the Smart Grid as well.

4.4.6 Authentication and Authorization of Users at Field Substations

Authentication and authorization of the personnel who work at the substation is an issue that needs research. Authentication and authorization should be provided in such a way that only intended users can be successfully authenticated to assigned devices and can only perform the relevant functions to the users. Authentication and authorization could help reduce the risks of unintended activities and malicious attacks, such as unintended modification of the configuration parameters and unauthorized access. Also, they could help mitigate the risks of insider attacks by the legitimate personnel, since the users can only perform minimum number of operations which they are allowed to.

The access to the IED's at the substations must be given to a specific user. Generally, it is given to a number of users having specific roles. These systems understand the meaning of the role but are not programmed to allow only the user who is assigned to that role. Therefore, it might be the case that passwords are shared among multiple maintenance personnel; although, the personnel may have different roles. Also, since there are many different devices deployed in a substation, the password that is shared may be common among many systems.

Moreover, the systems can be accessed locally or remotely. Accessing these systems remotely takes place over low speed communication lines. Hence carrying out authentication of the user can slow down the whole communication process. Therefore performing an authentication protocol such as RADIUS or LDAP is undesirable. Finally there should be some methods implemented which will authenticate and authorize during emergencies.

The needed research is to provide appropriate mechanisms or methods for user authentication and authorization at field substations in the smart grid systems that can tackle those issues specified above.

4.4.7 Key Management for Meters

Millions of smart meters will be eventually deployed in Smart Grid systems. To ensure security goals, cryptographic keys and other secret information must be contained in those meters in order to provide appropriate protection to AMI networks. Each meter should contain unique key or other secret information that could be used to generate or establish the keys based on the lifecycle of the key and also to protect the meter data from different kinds of attacks, such as eavesdropping, unauthorized modification, etc. Additionally, those keys and secret information contained in the meters need to be re-established and re-distributed at some appropriate point in time. The research on how those keys can be distributed and re-established and what mechanisms should be implemented in AMI systems are necessary. Thus, managing key materials for millions of meters are the potential problems. In some cases a large number of deployed meters may use the same symmetric or shared key across all the meters, perhaps in different states. Proper key management schemes should be implemented in such a way that the knowledge of one key should not result in the compromise of the entire system. Finally, since meters will be deployed across utility and AMI networks, the key management scheme should ensure that compromise of a key in one network will not affect the others.

The research in this area should cover all the aspects of the key management issues, such as cipher suites used and key sizes, key lifecycles, etc., which should be conformed to the NIST SP800-57 (Part 1)[173]. The research should also provide the solutions to the key distribution and key establishment issues for large scale systems.

4.4.8 Key Management for Wireless Sensor Networks

Wireless Sensor Networks are expected to be widely utilized in the Smart Grid, especially in Home Area Networks (HANs) and Neighborhood Area Networks (NANs). Sensors can be used to monitor physical properties, such as temperature, lighting and humidity, and convert the observed information into electrical signals which will be forwarded to EMCS or other devices. Once EMCS receives the sensor signals, it will determine the signals and shed or shift electric loads in homes or buildings. Therefore, to ensure security, sensor nodes must be able to authenticate each other and verify that the signals received have not been tampered with by anyone. Regardless of what schemes will be implemented, keys and secret information must be used in order to ensure security goals. However, sensor nodes have resource limitations, such as slow CPUs, short battery life and small amounts of memory. Thus, the secret information that could be embedded in the sensor nodes is limited due to small memories. Also, keys could be distributed over-the-air, thus there must be mechanisms to protect the keys as well. One of the communication protocols that could be used in wireless sensor networks is Zigbee protocol. The most concern in the Zigbee-based HAN network is the process of setting up a new device in the network because an attacker could connect his device in the Zigbee as well. Another issue is

---

[173] E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid; National Institution of Standard and Technologies (NIST), "Recommendation for Key Management – Part 1: General (revised)", March 08, 2007 [online]. Available: http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf

how the keys are established at both sides of the devices. When the new device is newly connected to the Zigbee network, the key must be established between the new device and its pair. The key distribution for each pair of nodes in Zigbee standard can be done by three methods as follows:

- Provisioning or Commissioning is to use out-of-bound mechanism, such as pre-installation key or over-the-air key, to place the key into devices. The key is sent over-the-air in plaintext, which is susceptible to one-time eavesdropping attack.
- Key Transport is to have a trust center distribute the keys to the devices. This method requires sending the key itself to the devices. The transportation of the key relies on the satisfactory security practice of the vendors. Thus, an attacker may be able to intercept the key, if the security mechanism for transporting the key is not secure enough to protect the key.
- Key Agreement is to have a trust center and devices negotiate the keys without transporting the key itself. Key Agreement is the most secure method for key establishment between devices in the network [174]. The key agreement is based on Symmetric Key Key Establishment (SKKE) which uses the master keys for distributing the shared secret key. However, the master key itself has the issue of the key distribution, since it has to be pre-installed or sent over-the-air.

Even though, Zigbee provides mechanisms for key establishment and key distribution, it still has some of the security issues specified above. Thus, to implement wireless sensor networks in Smart Grid systems, those issues need to be solved beforehand.

The research in this area should provide specific techniques or practices to protect the keys and also provide proper key management schemes that could be utilized in wireless sensor networks.

4.4.9 Side Channel Attacks

Cryptographic keys embedded into the equipment can be extracted using various attack schemes described in this section. Side channel attack is one of the attacks that are based on the information retrieved from devices that is not in the forms of plaintext to be encrypted or ciphertext from the encryption process. For example, encryption devices may produce timing information or power consumption statistics which may be predictable and can be exploited in order to predict the encryption techniques used by the device, the outcomes of the encryption process, or even reveal parts of the key using by the device. The information, such as timing information and power consumption statistic, obtained from these attacks is called side channel information and can be used to facilitate extraction of the entire cryptographic key. By carrying attacks based on timing measurements, power measurements, electromagnetic emission and faulty hardware side channel information can be retrieved.

---

[174] R. Cragie, "Public Key Cryptographic in Zigbee Network", Dec 2008. [online]. Available: http://www.elektroniknet.de/fileadmin/user_upload/pdf/euzdc2008/Cragie_Jennic.pdf.

- Power analysis attacks - This kind of attack basically involves analysis of the power differences in the signal and converting the trace into logical zeroes and ones in order to extract the key.
- Tempest attacks - This attack involves the principle that electronic devices such as monitors emit electromagnetic radiations during normal use. This can be obtained from a remote location using an antenna etc. and replaying the information thereby invading privacy.
- Timings attacks - In this type of attack the system is exploited by retrieving timing information which is obtained by examining the way in which inputs are processed by the system, including cryptographic keys.

The information gain from the side channel information along with other information gained by other methods could provide enough information that can be amplified to analyze and extract actual keys used. The research in this area is to come up with defense mechanisms that can be used to protect against those attacks.

4.4.10 Enhancing the Security of Serial Communication

Some legacy SCADA systems consist of serial communication links between the control centers and outstation devices. Most commonly used protocols on these serial links are DNP3 and modbus. They transmit text in unencrypted format and hence can be easily sniffed. Also solutions to enhance this such as wrapping protocols in IPSEC and SSL/TLS layer will put a load on these low bandwidth communication links and bring down the system speed to a large extent. This could impact the latency and bandwidth of communication and are not good solutions. Research is needed in order to find a mechanism which balances the speed of providing encryption and effect of encryption on the latency and bandwidth of the system.

4.4.11 Trust Management and Plug-in Hybrid Electric Vehicles

The Plug-in Hybrid Electric Vehicle (PHEV) network includes the vehicle owner's, utility (power generator) and retailer (power station similar to gas stations). There should be trust between all the parties involved in the PHEV network. To establish this trust, each component in the PHEV network which includes the communication network, power meters and secure payment features, should undergo rigorous testing for security flaws in the PHEV system. With continuous R&D, a proper solution needs to be drawn.

Figure 4-6 shows the basic components in a PHEV network. R&D will need to find an appropriate solution for PHEVs.

Figure 4-6: Basic PHEV Networks

The components are individually listed below:

1. Smart Meter: This component of the PHEV is one of the most important and complex components. It performs the task of a power meter. It also has the ability to communicate with the smart grid (utilities or SCADA systems) and other vehicles.
2. Vehicle to Grid (V2G): Vehicle to Grid capability, in simple terms means the ability of a vehicle to provide power to, as well as receive power from the electrical grid.
3. Vehicle to Vehicle (V2V): Vehicular Communication Systems are an emerging type of networks in which vehicles and roadside units are the communicating nodes; providing each other with information, such as safety warnings and traffic information. As a collaborative approach, vehicular communication systems can be efficient in avoiding accidents and traffic congestions rather than each vehicle trying to solve these problems individually.
4. Communication: The PHEV network is a wireless mesh which uses protocols such as Zigbee, WiFi and 3G for long distance communication. There are 2 types of communication divisions; V2G, a long distance communication, where the PHEV directly interacts with the SCADA system or the utility and V2V which are short range communications, around 1/2 a mile in range. In this type of communication, each PHEV communicates with other vehicles within the range, to identify the traffic flow.
5. Demand Response (DR): DR signals in a PHEV network change very quickly and drastically, depending on the demand of power for charging the vehicles, the grid must generate more power or schedule the vehicles for charging, such that they are able to adjust with the amount of power available. To perform these operations, a new system should be developed which can understand the demand and respond back to the vehicles by providing them power or scheduling an appropriate time. These systems are very complex and need to deal with real time demand response signals.

Figure 4-6 above shows the information flow between the different components of a PHEV network, each component must trust the information coming from the other component. An example would be best to explain the importance of trust in the PHEV network; for instance, if 1000 cars would start charging at the same instant, the grid would be unexpectedly overload,

which may cause the grid to fail. To prevent the grid from overloading, a SCADA-like system could send a signal to the PHEVs to inform them when to start charging and when to stop. This system would thus schedule each PHEV's charging time. Another such instance could occur if an attacker uses a reply attack and send a signal to all the PHEVs instructing them to start charging. They would instantly start charging, causing the grid to fail due to the over load. These are just simple scenarios in the PHEV network where trust is very important. In the PHEV network information flows between the PHEV, utilities, power retails and the billing system. This information flow takes place in different networks using different protocols. Establishing trust in the information flow between different components of the PHEV network is one of the most important areas where research needs to be done. Some of the existing systems that can be examined for ideas on how to do this are as follows:

- Billing systems in the gas stations - these systems have been secured and well maintained, to be able to manage the third party involvements, gas station companies in this respect;
- Online banking systems - this system is generally secure as it ensures confidentiality, integrity and availability of the data to the authorized individuals,
- Information flow through cellular communications - this system has well implemented cross domain communications;

The above mentioned systems are examples of systems that have been developed and improved over the years. Research should be done to identify how these systems ensure such high level security with the goal of using similar security measures to enhance the PHEV security.

4.4.12 Categorizing into Confidential and Non-confidential

The researchers do not consider any of the topics in this chapter to be confidential.

4.5 Wireless Communication Security

4.5.1 Security for Routing Protocols in Wireless Mesh Networks[175]

The two types of path determination (routing) techniques in wireless mesh networks (WMN) are proactive and reactive routing protocols. Proactive protocol is one which finds the path irrespective of the demand. Reactive protocols are those which find the path based on demand. There are threats associated with these routing protocols which might require knowledge about the routing protocols to inject erroneous packets to the network. The threats are summarized below:

- **Black-hole:** An attacker creates forged packets to imitate a valid node in the mesh network. The packets are attracted by advertising low cost routes and further attacking by dropping the packets.

[175] A. Geriks, J. Purcell, "A Survey of Wireless Mesh Networking Security Technology and Threats", SANS Institute, September 2006.

- **Grey-hole:** Forged packets are used by the attacker to drop packets, route and inspect network traffic.
- **Worm-hole:** Disruption of routing is carried out by replaying the routing control messages from one network location to another.
- **Route error injection:** An attacker by injecting erroneous packets to the mesh network can break the mesh links.

These threats greatly depend on the routing technology used. A proprietary routing protocol is less susceptible to these kinds of threats when compared to routing protocol like Ad-hoc On-Demand distance vector (AODV). These risks could be reduced by implementing message integrity checking for the routing messages and device authentication. Also, the routers in a mesh network are typically not power constrained but the clients which are mobile are power constrained. Hence there is a need of efficient routing mechanism for WMNs.

Research in this area is to secure the routing protocols, as wireless mesh networks are integral part of Smart Grid communication networks.

4.5.2 IEEE 802.15.4 Security Issues[176]

Asymmetric cryptographic algorithms like RSA and Diffie-Hellman use very long variables of sufficient length to ensure security. Sensor networks have very little memory and it is not sufficient to even hold these variables, let alone performing any operations on these variables. Also sensor networks have limited supply of energy. Hence the life span of a node is limited which in-turn limits the life span of a usable key. This hardware and energy constraint needs to be addressed and more efficient solutions need to be designed keeping the above constraints in mind.

To minimize the memory constraint and ease the management overhead, network-wide shared keying method was introduced. Here all the nodes in a network use a single key to communicate with one another. This takes care of memory requirement. But the key management becomes a problem since if a single node in a network is compromised, an adversary could use the compromised node to undermine the security guarantees of the entire network.

To avoid the problem with network-wide shared keying method, pair-wise keying was introduced. Here, pair of nodes in a network uses a unique key to establish a secure communication, this leads to management and memory overhead. As the number of nodes increase, each node's memory requirement and key management ability will also need to be upgraded.

A low cost solution to the keying methods discussed above was provided with a trade-off between network-wide shared keying and pair-wise keying, with partial resistance to node compromise. Here a common key was used to establish secure communication between a set of

[176] I. Ghansah, "Smart Grid Cyber Security Potential Threats, Vulnerabilities and Risk", California Energy Commission, PIER Energy‐Related Environmental Research Program. CEC‐500‐2008‐027, October 2009.

nodes belonging to a group. These nodes are grouped based on the location, network topology and other similar functions.

The above mentioned solutions are summarized by the following examples:

1. If a key is used in multiple ACL entries then it is likely to reuse a nonce value (unique key used for encryption), in which case confidentiality can easily be broken. For example, if a user sends a message m1 with a nonce value x1 to recipient r1 and then sends a message m2 with the same nonce value x1 to recipient r2, the adversary can retrieve the message as show below[177].

   $$(m1 \oplus E_k(x1)) \oplus (m2 \oplus E_k(x1)) = m1 \oplus m2,$$

   where E_k denotes encryption of the data using key k
2. Network-wide shared key is incompatible with replay protection. For example, if user A sends 100 messages to recipient r1, the replay counter would be incremented from 0 to 99 at the receiver's end. Now if user B sends a message to recipient r1 with a replay counter 0, the recipient r1 rejects the message as its replay counter has been incremented and is no longer 0. Recipient r1 would only accept a message from user B if the replay counter value of the message is greater than 99. To overcome such issues, there has to be some form of co-ordination between the nodes in the replay counter space. This would not be feasible when the node density increases.

Thus working on finding a solution that would solve the problem of the ACL tables' inability to support different keying models is required in IEEE 802.15.4.

4.5.3 Categorizing into Confidential and Non-Confidential

The researchers do not consider any of the R&D topics in this chapter to be confidential.

[177] N. Shastry, D. Wagner; UC Berkley., "Security Considerations for IEEE 802.15.4 Networks", Year of Publication – 2004.

CHAPTER 5:
Privacy In The Smart Grid

5.1 Introduction

Smart Grid is a system of systems and a network of networks with a high degree of complexity. Its supporting infrastructure will collect consumer's energy usage information at a high level of accuracy. While the reasons for collecting such high resolution data are compelling, it is judicious to examine the type of data collected and how it will be managed and protected.

The information collected by utilities via smart meter can potentially detail the consumers' energy consumption use and patterns within the homes exposing private activities to anyone with access to this sensitive and personal information. Further, smart meter energy data are transmitted via potentially insecure communication channels, and stored in databases which could be accessible remotely by consumers, utilities, and third party service providers.

Such exposure of sensitive information would constitute invasion of consumers' privacy. While there are benefits of providing consumers more control over their energy usage and utilities should provide means of meeting this marketplace demand response, the utilization of meter data must be done in a trustworthy fashion.

The Supreme Court has upheld the sanctity of the home as the touchstone for privacy protection, however business records implies that consumer elected to transact with the business and to engage in activities open to observation by the business and therefore are unprotected by the Fourth Amendment. In the light of this definition, smart meter data has been treated as business records and therefore is unprotected under the Fourth Amendment.

To avert possible abuse to consumer rights the relationship between consumer and Smart Grid entities must be covered by privacy laws and regulations. Are the existing privacy laws adequate to protect Smart Grid consumers?

This document addresses the privacy issues associated with information gathered within the Smart Grid. What measures must be taken to ensure consumer privacy is not violated? What current laws and technological framework can be applied to Smart Grid data and do they suffice? How the benefit that Smart Grid will provide be balanced with the preservation of citizens' or businesses rights to their privacy?

5.1.1 Overview of Privacy

5.1.1.1 Definition

Privacy is both a legal and an ethical issue. Privacy can be defined as the ability of an individual or group to seclude information about them thereby reveal themselves selectively. In other words an individual has the right to control who knows certain aspects about them, their communications, and their activity and thus differ from confidentiality which is defined as access to information should be limited to only those with a business need to know. Privacy can be related to anonymity, meaning the desire to remain unidentified in the public realm.

The boundaries and content of what is considered private differ among cultures and individuals, but share basic common themes. In many nations privacy laws or even constitutions protect citizens against unsanctioned invasion of privacy by the government, corporations or individuals. Privacy may be voluntarily sacrificed, normally in exchange for perceived benefits and very often with specific dangers and losses, although this is a very strategic view of human relationships.

Information privacy can mean different things to different individuals, groups and organizations. In essence privacy is an aspect of security and includes the concepts of appropriate use and protection of information and just as confidentiality, integrity, and availability can conflict, so can privacy. The three aspects to information privacy are sensitive data, affected parties, and controlled disclosure.

5.1.1.2 Definition

Privacy issues existed long before computers and networks however they have without a doubt affected the feasibility of unwanted disclosure due to the enormous computer storage capacity and speed. Rezgui et al[178] defined the eight dimensions of privacy as:

1. Information collection - Data Collection with knowledge and explicit consent only.
2. Information Usage - Data used for specified purposes only.
3. Information Retention - Data are retained (stored) for a specified period of time only.
4. Information Disclosure - Data are disclosed to authorize entities only.
5. Information Security - Utilization of approved mechanisms to ensure data protection.
6. Access Control - Control all modes of access to all forms of collected data.
7. Monitoring - Maintain logs for all data access.
8. Policy Changes - More permissive security policies are never applied after the fact to already obtained data.

5.1.1.3 Principles

U.S. Laws and regulations on privacy issues are based on the fair information practice principles which covers the eight dimensions of privacy[179] are defined as:

1. Collection Limitation - Lawful and fair collection of data
2. Data Quality - Relevant data must be relevant, accurate, complete and up-to-data
3. Purpose Specification - Purpose for data usage must be specified and data must be destroyed when it no longer serve the purpose.

---

[178] Rezgui, A., et al, "Privacy on the Web: Facts, Challenges, and Solutions." IEEE Security & Privacy, v1 n6, Nov2005, p40-49

[179] WAR73a, Ware, W. "Records, Computers and the Rights of Citizens." RAND Technical Report, p-5077, Aug 1973

4. Use Limitation - Authorization by data subject or authority of law for all other unspecified purposes.
5. Security Safeguards - Establish procedures to protect against data loss, corruption, destruction or misuse.
6. Openness - A data subject should be given capability to acquire information about collection, use and storage of his/her personal data systems.
7. Individual Participation - data subject has the right to access and challenge the accuracy of his/her personal information.
8. Accountability - A designated data controller should be held accountable for the compliance with the measures to give effect to the principles.

5.1.1.4 Generally Accepted Privacy Principles (GAPP)

The GAPP forms the basis of most international, national and local data protection laws, with safeguards as those used for data protection found in the international information security Standard ISO/TEC 27001[180]

1. Management and Accountability: An organization should formally appoint personnel to ensure that information security and privacy policies and practices exist and are followed. Documented requirements for regular training and ongoing awareness activities should exist and be followed. Audit functions should be present to monitor all data accesses and modifications.
2. Notice and Purpose: A clearly specified notice should exist to describe the purpose for the collection, use, retention, and sharing of Personally Identifiable Information (PII) see Appendix B for detail definition. Data subjects should be told this information at or before the time of collection.
3. Choice and Consent: The organization should describe the choices available to individuals and obtain explicit consent if possible, or implied consent when this is not feasible, with respect to the collection, use, and disclosure of their PII.
4. Collection and Scope: Only PII that is required to fulfill the stated purpose should be collected from individuals. Treatment of the information must conform to fair information processing practices. Information should be collected directly from each individual person unless there are justifiable reasons why this is not possible.
5. Use and Retention: Information should only be used or disclosed for the purpose for which it was collected, and should only be divulged to those parties authorized to receive it. PII should be aggregated or anonymized wherever possible to limit the potential for computer matching of records. PII should only be kept as long as is necessary to fulfill the purposes for which it was collected.
6. Individual Access: Organizations should provide a process for PII data subjects to allow them to ask to see their corresponding PII and to request the correction of perceived

[180] NIST7628 guidelines for Smart Grid Cyber Security, Aug 2010

inaccuracies. PII data subjects must also be informed about parties with whom PII has been shared.

7. Disclosure and Limiting Use: PII should be used only for the purposes for which it was collected. PII should not be disclosed to any Other-parties except for those identified in the notice, or with the explicit consent of the individual.
8. Security and Safeguards: PII, in all forms, must be protected from loss, theft, unauthorized access, disclosure, copying, use, or modification.
9. Accuracy and Quality: Every effort should be made to ensure that the PII is accurate, complete, and relevant for the purposes identified in the notice, and remains accurate throughout the life of the PII while within the control of the organization.
10. Openness, Monitoring and Challenging Compliance: Privacy policies should be made available to PII data subjects. PII data subjects should be given the ability and process to challenge an organization's compliance with their state privacy policies as well as their actual privacy practices.

5.1.1.5 Laws and Regulations

The following is a list of U.S. data protection laws[181]

1. 1974 Privacy Act - This law applies only to data maintained by the U.S. Government and includes most of the Principles of Fair Information Practices and is the strongest law due to its breadth and applies to all personal data held anywhere in the Government.
2. Health Insurance Portability and Accountability Act - Known as HIPPAA addresses the consumer healthcare information.
3. Gramm-Leach-Bliley Act - Known as GLBA and addresses consumer financial service organization.
4. Children's Online Privacy Act - Known as COPPA and addresses children web access
5. Electronic Communication Privacy Act 1986 - known as ECPA set provisions for access, use, disclosure, interception and privacy protections of electronic communications.
6. Fair Credit Reporting Act - Known FCRA. This law addresses the consumer credit data. It protects data collected by non-government organizations.
7. Federal Educational Right Act - Known as FERPA protects student records
8. e- Government Act - Requires all Federal Government Agencies to post privacy policies on their web sites. The policies must disclose the following:

[181] Panusuwan, V.et al."Privacy Risk assessment Case Studies Support of Square.", Jul 2009

- The information to be collected
- The purpose for the collected information
- The entities to whom the information will be disclosed
- Notice or consent opportunity to users regarding what information is collected and how if any of it is shared.
- Disclose how the user information is secured.
- Inform user of their rights under the Privacy Act and any other relevant laws protecting the user privacy.

9. The Patient Safety and Quality Improvement Act of 2005
10. Fair Information Practices Act (FIPA)
11. The California SB1386 law - Breach Notification It requires any company doing business in California or any California government agency to notify individuals of any privacy breach that has or has reasonably believed have compromised personal information of any California resident.

5.2 Privacy in Smart Grid

Smart Grid is the modernization of the electric grid and transforming it to a bi-directional flow of information and electricity. Its' infrastructure will be capable of informing consumers of their day-to-day energy usage down to appliance level. The Smart Grid will be driven by communications technology and infrastructure collating data provided by smart meters, sensors, computer systems into comprehensible and actionable information for both consumers and utilities.

5.2.1 Behind Smart Meter Data Collection

There are many reasons behind the collection of consumer's electricity consumption that are compelling, but the challenge here is at how the data will be managed and protected. To be capable of meeting demand response and to enhance the load management, utilities need better load modeling methods which would require more detailed information. Real-time information gives utilities the ability to monitor loads and adjust to unexpected load changes.

The more refined the information collected the more responsive the grid would be to load demand. On the consumer end information will be collected by Smart Meters from smart appliances, thermostat and the PHEV.

Both climate change and energy security drive the move toward lowering emissions, this meant incorporating renewable resources such as wind and solar power. These resources will allow a better distributed grid by matching load demand locally and reduce energy loss over long transmission lines.

The drive to change the utility's billing structure from a constant to variable rate. There are various schemes ranging from a basic two rate scheme to a more dynamic scheme (with the most saving benefit to consumers) where the rate changes from minute to minute.

Managing the demand side by provide consumers with detailed information about their energy consumption to draw attention to the low-level constant draws (and its' cost) when managed would reduce the energy usage and therefore emissions.

Plug-in Hybrid Electric Vehicles (PHEV) would contribute to solving both environment and energy security issues by harnessing the un-utilized energy generated from existing power plants. PHEV load would be managed by utilizing the valleys of load demand without generating new peaks and thus effectively reducing emissions and oil dependency.

5.2.2 Smart Meter Data

In Smart Grid data will flow back and forth between utilities and consumers residence. Figure 5-1 indicates the specific data items involved and the associated privacy issues. The data items collected from the DER and Smart Meter will reveal information and activities within the home or business.

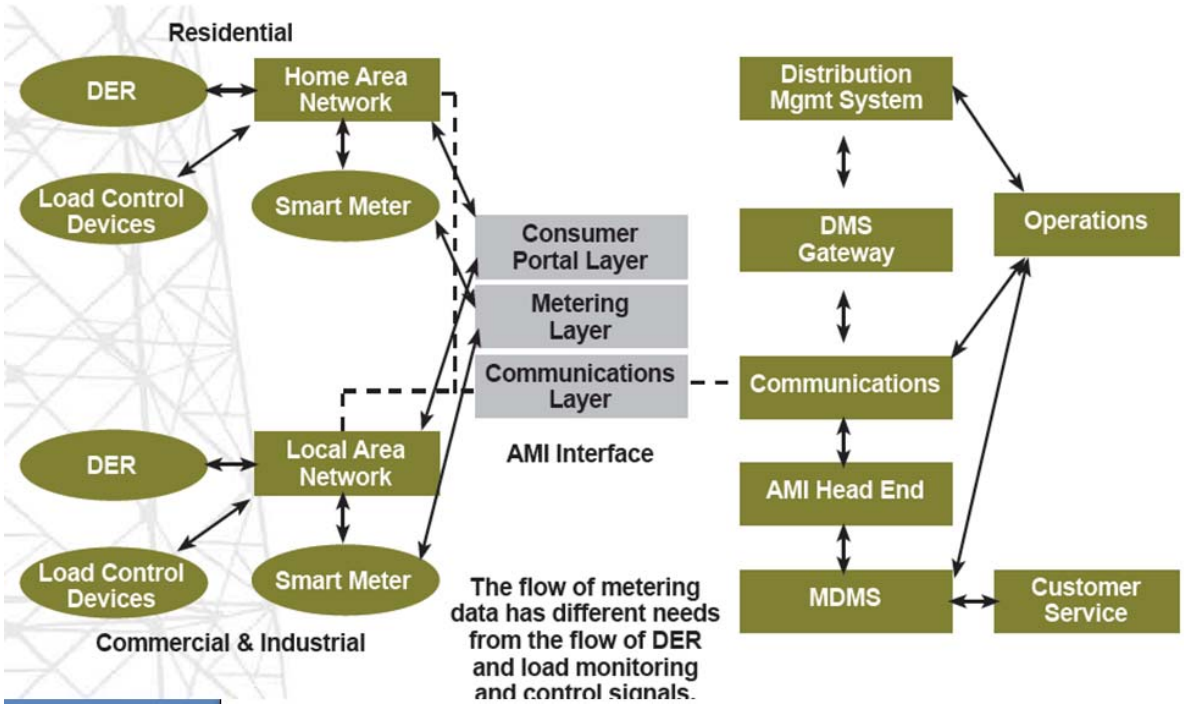


Figure 5-1: Data Flow of residential and commercial Meter Data[182]

[182] National Energy Technology Laboratory (NETL), Advanced Metering Infrastructure, February 2008

Table 5-1: Summarizes the different ways consumers would interface with Smart Grid to manage their energy usage

Consumer Activity	Consumer Activity Detail
Understand household energy use	Log into their energy usage account and review their usage real-time as it is reported by their smart meter
Manage energy use	Consumer's smart appliances could be programmed to run at cheaper rates times.
Reduce Carbon footprint	At peak energy usage time, allow energy to lower consumption by adjusting heating/cooling and delaying the use of other appliances till off peak time (such as dish washers, washing machines, etc.)
Control Electric Expenditure	Consumers review their energy consumption daily and the contribution of different appliances to their energy cost.
Experience fewer Power Outages	Smart Grid ability to pinpoint outage location allowing utilities to dispatch repair crew efficiently and re-route power delivery to affected area.
Receive Notification for estimated resumed service	Consumer can sign up to receive notification of power outage via text messages.
Control household electricity	Tying in all consumer's energy devices capable of giving energy back to the grid such as plug-in vehicles and solar panels to the household control, which will provide real-time indication of energy use. Consumers can monitor their household net energy usage and be able to adjust devices to lower usage. Consumers can monitor and control household smart devices remotely.

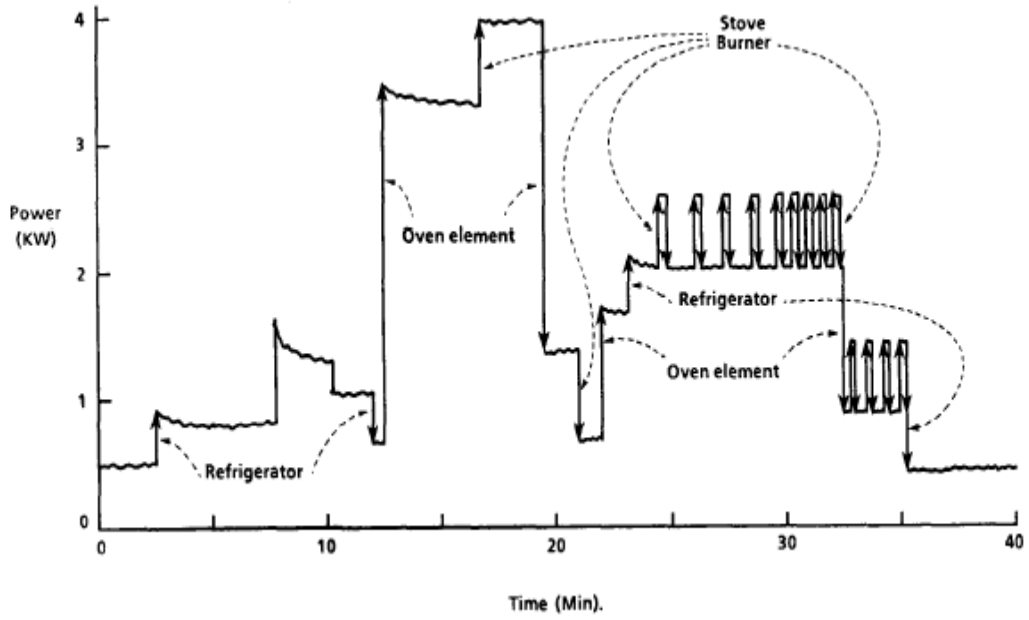
5.2.3 Characteristics of Smart Meter Data

There are two research fields concerned with electricity consumption and load management. First is the empirical research and load monitoring carried out by Non-intrusive Appliance Load Monitoring (NALM) and the second is the development of mathematical methods utilizing artificial neural networks to glean detailed usage information from low resolution interval data (Smart Meter).

The idea behind the NALM project was driven by the fact that appliance data collected in a laboratory differed from the data collect in real-time in homes. George Hart and Fred Schweppe developed the NALM which consist of a hardware and software components to collect appliances load signatures. Figure 2 shows the load signatures for various appliances. The hardware device is attached to an existing metering infrastructure and allowed real-time collection of electricity usage. It handles the edge detection and data transmission. The software performs the signal processing analysis. Today, because of the NALM technology most major appliances by make and model load signatures have been cataloged into a library and efforts are underway to catalog small appliances.

The data collected by the Smart meter is of lower resolution compared to the data collected by NALM, however by using inductive algorithms and mathematical methods the gap between them is closing.

Figure 5-2: Different Appliance Load Signatures183



5.2.4 Smart Meter Data and its' Implications

In the Smart meter, the information capture is increasing in granularity, and thus consumer's electricity usage profile can reveal intimate details about the activities inside a consumer's home. Figure 3 shows the energy usage profile of a consumer in a 24 hour period.

This data if viewed as grid data alone within a centralized server, it would not reveal a specific consumer or household. However, if combined with the consumer Personally Identifiable Information (PII), such as address or meter identification it would raise serious privacy concerns. Also, roaming Smart Grid devices such as the PHEV, adds more additional flow of the consumer's PII and derived PII.

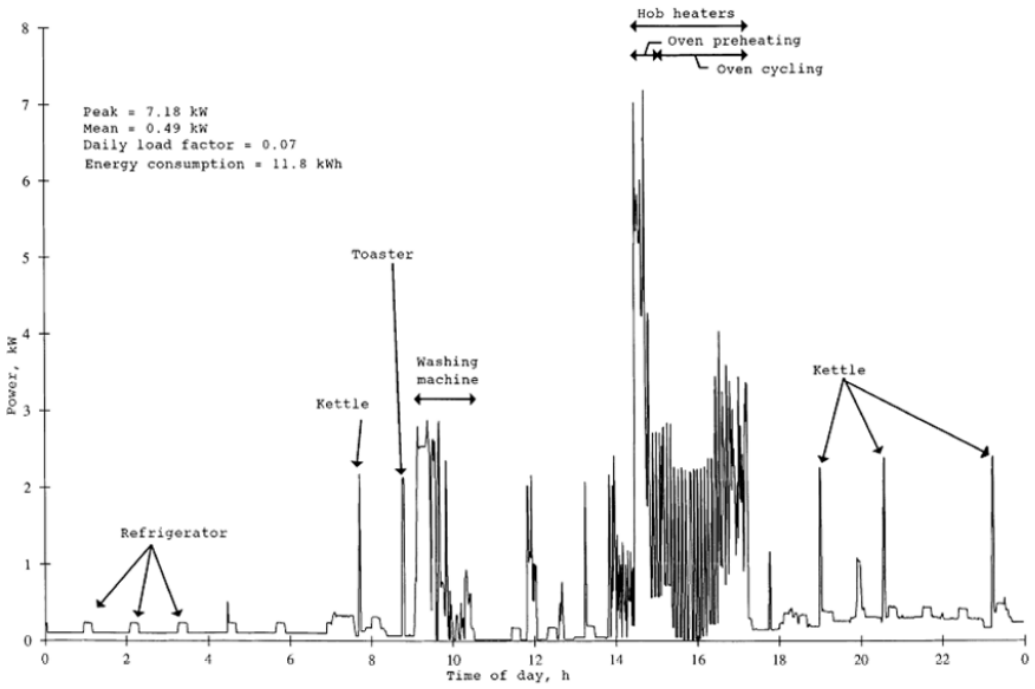
The potential for gleaning private information from Smart Meter data is staggering and can reveals intimate details about activity inside a customer's house including when they are home, sleep, eat, watch TV, own an alarm and if they use it, etc.

Consumer's electricity usage profile, can identify use of specific appliances within the homes, and pinpoint exactly where within the home those appliances are located. The wealth of information from the Smart Meter gives rise to troublesome uses for such data.

---

[183] Drenker & Kader, at 1871

Figure 5-3: Household Electricity Demand Profile Recorded in a 24 hour[184,185]



5.2.5 Smart Meter Data and Disclosure Risks

For the utilities, the Smart Meters' real worth lies in the information generated. Utilities may wish to sell collected usage information to marketing agencies or other interest parties, a practice proven to be quite lucrative in e-commerce.

The gathered usage profile has the potential of becoming a source of behavioral information on a granular level that consumers may regard as private or prefer it remains secret.

Although, there are positive aspects for the utilities which include their ability to spot thieves who intermittently bypass the meters and steal power, or analyzing data to pinpoint customers whose consumption is falling inexplicably, a sign of a failing meter that needs replacement, there are more scenarios that raise privacy concerns.

---

[184] G. Wood & M Newborough, Dynamic Energy-consumption Indicators for Domestic Appliances: Environment, Behavior, and Design, 35 Energy and Buildings 821, 822 (2003) (citing M. Newborough & P. Augood, Demand-side Management Opportunities for the UK Domestic Sector, IEEE Proceedings of Generation Transmission and Distribution 146 (1999) 283-293)

[185] Elias Leake Quinn, Smart Metering & Privacy: Existing Laws and Competing Policies, Spring 2009

Energy usage information disclosures if accessible to:

1. Political entity/media could lead to social embarrassment, such was the case - The day after Al Gore's climate-change documentary, "An Inconvenient Truth", received an Oscar, Tennessee political activists released the purloined electric billings for Gore's Nashville mansion to embarrass him - his usage was nearly 20 times the national average.
2. Law enforcement could lead to prosecution of individuals, such as the case - When experts discern the telltale signs of illicit activity, such as a marijuana" grow house (even though this is a good outcome under the law the consumer should be granted privacy in their home).
3. Divorce lawyer sifting through the meter data and asking: how were the children left home alone in a custody battle.
4. Appliance manufacturer or insurance agent: who could question the usage of an appliance/behavior of a consumer and invalidate an appliance warranty or decline insurance coverage.
5. Inconspicuous characters could lead to Identity theft, or home invasion or other situation not even dreamt of yet.

In addition, energy use itself has become synonymous with an individual's social responsibility, and so, intuitions about the private nature of this data may lead to be more protective of its disclosure.

Derived data can also cause privacy concerns. Table 2 shows the various types of derived information from the Smart Meter data and the various risks associated with each.

Table 5-2: Privacy concerns, associated risks and potential use of data

Privacy Concern	Type of Risk	Specific Potential Use of Data
Combinational PII		Identity Theft Accidental Invasion
Use Profile	Determine Personal Behavior Patterns Activity Censorship	Target Marketing Affect Insurance coverage (Health, car, or home Could be used by government to tax certain activities Malicious Intent (blackmail) Could be used by government, or law enforcement or media to cause harassment, social embarrassment damaging actions
Use of Specific Smart Appliances	Usage Censorship	Could lead to invalidate appliance warranties Could determine approval/decline of insurance claims
Real Time Surveillance	Decisions and Actions based on inaccurate consumer information stored in the utilities database	Target Marketing Target home Invasion

Data Access	Upon change of Smart Meter ownership, if consumer information inaccurate Data Access consumer	Potentially, consumer PII data will become inappropriately modified Affect automated Smart Grid decisions made for consumer energy use Lead to stored use profile and activities inaccurately
Residual Meter Data	Upon change of Smart Meter ownership, Reveal prior Smart meter owner activities	Reveal prior Smart Meter owner activities and usage causing that consumer violation of privacy and subject to Identity Theft, malicious intent, .etc.

As demonstrate above, the privacy implications are astounding, and the risks of disclosure must be addressed.

5.2.6 Smart Meter and Privacy Law

The disclosure risks pegs the question is interval data of electricity consumption (Smart Meter Data) protected under the umbrella of privacy law?

The Supreme Court has upheld the sanctity of the home as the touchstone for privacy protection, however business records collected by third parties have fewer privacy protections stemming from the theory that consumer elected to transact with the business and to engage in activities open to observation by the public and therefore are unprotected by the Fourth Amendment.

In the light of the above definitions, electric metering information has been treated as business records and therefore is unprotected under the Fourth Amendment despite the fact that it contains intimate details of the in-home activities of the consumer.

In addition, there are no formal privacy policies, standards or procedures for data collection throughout the Smart Grid have been implemented or proposed by any state utility commissions.

There is no comprehensive and consistent definition of "Personally Identifiable Information" (PII) among state regulations. In one definition PII can be defined as any information that is about, or can be related to, an identifiable individual. It includes any information that can be linked to an individual or used to directly or indirectly identify an individual or can be attributed to an identified individual.

Utilities can potentially extend their services across state line or country borders and in a free market environment ownership of utility enterprises can be bought and sold to foreign entities and hence adds an international consideration.

All of the above reasons highlight that the lack of consistency and comprehensive privacy policies would lead to significant privacy risk that required regulatory measures to address these privacy issues.

5.2.7 Addressing Privacy Concerns in the Smart Grid

With the passing of the EISA law, the National Institute of Technology (NIST) was assigned "primary responsibility to coordinate development of a framework to include protocols and

model standards for information management to achieve interoperability of Smart Grid devices and systems."

The privacy implications of the Smart Grid at best are undefined, that led NIST to appoint a privacy Sub-group of the Cyber Security Coordination Task Group to performed a high-level Privacy Impact Assessment (PIA), of the privacy implications regarding the consumer-to-utility type and amount of information flowing through the various entities of the Smart Grid, the risks posed by "anonymized" data aggregation and the frequency of consumers' collected data that potentially could be real-time surveillance." They also examined the laws and regulations relevant to the privacy of the consumers' information collected by Smart Meters. They published their findings in NIST7628.

NIST Consumer-to-Utility High-Level Privacy Impact Assessment (PIA)[186]

The PIA was developed in accordance with the Generally Accepted Privacy Principles (GAPP) on which most international, national and local data protection laws are based and ISO/IEC 27001 International Information Security Standard (that defines information Security Management System Standard) as the foundation for its recommendation and tailored it to Smart Grid Privacy Issues. Under the GAPP, privacy is defined as "the rights and obligations of individuals and organizations with respect to the collection, use, retention, and disclosure of personal information." For Smart Grid NIST 7628 viewed privacy as:

1. **Privacy of personal information.** Personal information describes specific aspects of an individual and is the most known dimension of privacy. It means an individual has the right to control when, where, how, to who, and to what extend he/she shares his/her personal information, to access personal information given to others as well as the right to correct it, and ensure it is safeguarded or disposed of appropriately.
2. **Privacy of the person.** Personal privacy is the right to control the integrity of an individual's own body.
3. **Privacy of personal behavior.** Behavioral privacy is the right of individuals to make their own choices about what they do, such as political, sexual, or religious activities, and to keep certain personal behaviors from being shared with others.
4. **Privacy of personal communications.** Personal communications privacy is the right to communicate without undue surveillance, monitoring or censorship.

In the high-level PIA the task Group concluded that there is a "lack of consistent and comprehensive privacy policies, standards and supporting procedures throughout the states, government agencies, utility companies, and supporting entities that will be involved with Smart Grid management and information collection and use creates a very significant privacy risk that must be addressed"

---

[186] NIST7628 guidelines for Smart Grid Cyber Security

PIA stated the following:

1. The privacy implications of Smart Grid are not fully understood.
2. Lack of formal privacy policies, or standards set by Smart Grid entities
3. Utilities have no comprehensive and consistent definition or Personally Identifiable Information.
4. Distributed energy resources and smart meters will reveal data about consumer home activities.
5. Consumer PII can be used in unlimited ways

The privacy principles reviewed in the PIA were management and accountability; notice and purpose, choice and consent; collection and scope; use and retention; individual access; disclosure and limiting use; security and safeguards; accuracy and quality; openness, monitoring and challenging compliance.

The task group recommendations in the PIA document were stronger than that of ISO/IEC 27001. It highlights the need to establish POLICIES & STANDARDS with regard to consumers' information within the various Smart Grid systems.

To Establish:

1. A Smart Grid agency responsible for the oversight and standard enforcement of the Smart Grid privacy policy.
2. Smart Grid Privacy Policy defining consumer privacy rights, Personal Identifiable Information (PII) and derived PII.
3. A definition of privacy protection standards. A definition of what constitutes a privacy breach of PII within the Smart Grid System. Privacy breach protocol that must be followed by all Smart Grid Entities.

To Establish Policies and Standards for:

1. PII storage repositories and accessibility throughout all areas of Smart Grid that must be followed by all utilities and third parties with Grid access.
2. Ensuring entities involved with implementing or maintaining consumer Smart Grid and meter data receive regular training.
3. The types of privacy notices and content that utilities must provide to consumers.
4. Publicly available location (web) where consumer can find information about the types and purpose of PII collected used.
5. The types of service choices that utilities must provide to consumers
6. Utilities to follow to obtain consent before sharing residential PII with other entities.
7. Specify the types of data items that can be collected through Smart Meters.
8. Utilities to collect only the specified data.

9. Outlining the appropriate and acceptable uses for the collected data items from all possible Smart Grid devices.
10. Specifying the retention duration of each type of meter data.
11. Mechanisms to effectively and irreversibly remove meter data from Smart Grid devices and residential Smart Meters.
12. Providing consumers access to their stored PII data items within all Smart Grid Systems.
13. Ensuring that third party entities storing consumer's data must follow all the established P&S defined here.
14. Notifying consumers whenever their PII is shared with a third party.
15. Clear definition of how PII and derived PII within all areas of SMART Grid can and cannot be used.
16. Consumer ability to file complaints

Smart Privacy for Smart Grid[187]

Ann Cavoukian, developed the concept of Privacy by Design. The objective of this approach is to ensure the privacy and control over one's information at the same time business entities maintain a competitive advantage.

In her approach, she defines the term Smart Privacy to encapsulate law, regulations, accountability & transparency, data security to ensure that all personal information held by an organization is appropriately managed.

Utilizing her approach, she incorporated the regulatory recommendations in the PIA directly into the Smart Grid by means of making privacy the default in all aspects of Smart Grid System.

A summary of her proposed approach to Smart Grid Design pertaining to consumer-to-utility information is:

1. Collect the minimum customer Personal Information (PI) without compromising services offered.
2. Transparent communication with customers regarding their PI collected, it use, disclosure, and retention and allowing consumer to tailor their PI options based on their preference.
3. Securely disposes of consumer PI when it is no longer needed for the purpose for which it was original collected.
4. Proactively obtain consumer consent before disclosing their PI with a third party.
5. Deliver accurate information and allow consumers to correct their PI if necessary.

---

[187] Cavoukian, A. "SmartPrivacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation", Nov 2009

6. Resistant to data leakage, reinforced with privacy by default and breach notification protocol.
7. Gain customer trust would foster customer participation.

5.3 Best Practice for Protection against Privacy Loss in Smart Grid

NIST Recommendations for mitigating Privacy Concerns[9]

All entities involved in Smart Grid should follow the NIST 7628 recommendations for mitigating Privacy Concerns within the Smart Grid by

1. Conduct a privacy impact assessment (PIA) to identify risks to the personal information (PI) that can potentially be collected, processed, stored and handled. Smart Grid entities could utilize the NIST methodology to do their own PIAs. To perform a PIA an entity should

    a. Conduct an initial PIA to establish a baseline privacy posture

    b. Subsequent PIAs should be performed whenever there is a major change that could potentially raises or new privacy concerns.

2. Develop privacy policies and practices document utilizing OECD Fair Information Principles. In particular, the Privacy Group recommends the following practices (see Appendix A).

    Use software engineering principles to develop privacy use cases as a mechanism to track data flows and privacy implications of the collected data.

3. Provide consumers with information regarding the risks to their privacy within Smart Grid and provides means to mitigate them.

4. Collaboration and information sharing between Smart Grid market participants are vital for data protection (see Appendix B on collaboration).

    Manufacturers and vendors of smart meters, smart appliances, and other types of smart devices, should collect the minimum possible amount of data necessary for the purposes of the smart device operations following OECD Fair Information Principles (see Appendix A).

Smart Privacy as Design Concept

Utilize Privacy by Design principles developed by Ann Cavoukian, which are:

1. Proactive not Reactive – To anticipate and prevent privacy invasion before they occur.
2. Privacy as the Default – To ensure the maximum degree of privacy by automatically protecting personal data in any given IT system
3. Privacy Embedded into Design – Embedding privacy into the design and architecture of IT system and business practices.
4. Full Functionality – To provide privacy without sacrificing security
5. End-to-End Lifecycle Protection – To ensure that privacy by design is embedded into IT system and is being extended throughout the lifecycle including the data destruction at the end of its pre-established retention period.
6. Visibility and Transparency – All Smart Grid entities operate according to stated objectives that subject to independent verification.
7. Respect for User Privacy – Mandate that architects and operators provide measures for strong privacy defaults, appropriate notice and user-friendly mechanisms.

Data Governance[188]

Data governance is an organization's implementation of policies and process to achieve:

1. Maximize the value of data
2. Manage what data to be collected
3. Determine data usage to accomplish organization's goals.
4. Address compliance requirements such as statutes, regulations and laws.
5. Mange risks of storing personal information (PI).

An organization's data governance investments provide the organization with competitive advantages as well as risk reduction. Controls used to fulfill compliance requirements can lead to improvement of the organization performance, and implementing data retention restrictions saves storage and maintenance costs which results in efficient resource utilization.

The process of analyzing the flow of information throughout an organization, how and who accesses it and for what purpose allows an organization to determine where to implement mechanisms to protect personal information (PI). The information life cycle consists of phases and actions that an organization can utilize to address its data governance considerations. It is composed of:

- **Collect:** Establish controls to ensure compliance with privacy policies for all collected PI. Organizations must determine their administration of their privacy policies over the lifespan of the information.

[188] Managing and Protecting Personal Information", A Microsoft Perspective on Data Governance for Privacy and Compliance for the Enterprise, Feb 2009

- **Data Storage:** Utilization of storage controls mechanisms to protect information stored and shared.
- **Update:** Implement data integrity using processes to ensure that data is accurate and current throughout its lifespan.
- **Process:** Ensure that only authorized personnel have access to sensitive or critical information.
- **Delete:** Minimize risks from data breach by setting a finite lifespan for sensitive data by enforcing automatic deletion and/or secure archiving.
- **Transfer:** Extend all organization privacy and data integrity processes to transferred sensitive data.

The concepts of Governance, Risk and Compliance (GRC) are used by organizations to mitigate issues ranging from compliance with regulation requirements to accomplish information security and customer privacy. Data governance is the cornerstone to the implementation of a comprehensive and complete GRC and understanding the information life cycle is vital to an organization's data governance implementation and success.

A framework to manage GRC requires:

1. The deployment of an IT infrastructure to safeguard and manage PI to prevent unauthorized disclosure by continually assessing data risks and deploying security controls to meet organization's information needs.
2. Use of authentication mechanisms to verify user's identity to ensure only legitimate users can access systems resources and data appropriately by observing the principles of the Seven Laws of Identity which states:
    - Reveal information identifying a user only with that user's consent
    - Disclose the minimum amount of information necessary to facilitate identification
    - Limit identifying information to parties with necessary and justifiable need to access.
    - Provide public entities with the use of "omnidirectional" identifiers and private entities a "unidirectional" one.
    - Use and interoperate with multiple identity technologies and providers
    - Develop user interface with mechanisms to protect against identity attacks
    - Guarantee users a simple, consistent access process.
3. Safeguard organization's PI using encryption methods for protection against interception and viewing of PI by unauthorized parties throughout the PI lifecycle to meet legal and regulatory requirements with respect to management and retention of all sensitive information

4. Deploy monitoring processes to perform audit and reporting to assist in verifying system and data access controls are operating effectively and identify suspicious or noncompliant activity.

Apply the Eight dimensions of privacy to all Smart Grid consumers PII.

Use the Privacy Principles and Policies: Fair Information Policies throughout the Smart Grid Life Cycle.

Privacy-Preservation[189]

The FCC technology and privacy Advisory Committee recommendations against privacy loss are:

1. Data Minimization - Collect the least data for the task.
2. Data Anonymization - Use mechanisms to prevent data linkage.
3. Audit Trail - Keep records as to who and when data was accessed in event of a privacy breach.
4. Security and controlled Access - Take adequate measure to protect and control access to personal information.
5. Training - Ensure personnel who access sensitive data understand why and how to protect personal information.
6. Quality - Data usefulness is determined by the purpose for which data was collected, its storage, its age.
7. Restricted Usage - Determine if uses of the data is consistent with the purpose for which it was collected.
8. Policy - Develop and enforce a clear Privacy Policy

Ensure that privacy policies include ways to safeguard consumer private data by utilizing ways to protect against privacy loss.

Data Access Risks [190]

Utilize mechanisms to eliminate Data Access Risks to consumer information

The risks associate with the acquisition of data from other entities can be categorized as follow:

1. Data errors -Refers to all errors from data entry to data analysis.
2. Inaccurate Linking - When correct data items are erroneously linked on a common element.
3. Difference of form/content - Encompass precision, accuracy, format, and semantic errors.
4. Purposely wrong - Data collected from sources that intentionally provide erroneous data to mislead.
5. False Positive - Outdated or incorrect data with no mechanism in place to verify or reject it.
6. Mission Creep - Collected data used for more than its' intended use.

---

[189] Technology and Privacy Advisory Committee to the DoD. Safeguarding Privacy in the Fight Against Terrorism.", committee report, 1 Mar 2004

[190] Technology and Privacy Advisory Committee to the DoD. Safeguarding Privacy in the Fight Against Terrorism.", committee report, 1 Mar 2004

7. Poorly protected - Poor management of data that compromise its' integrity.

Privacy on the Web

Anonymity on the web is superficial at best and sophisticated web applications collect a lot of user's information. The following are few examples of the privacy risks on the web

Internet Authentication- Confirms the user's identity and not the server.

Credit card- Payment on the internet protects the merchant only consumer's information once given to one merchant becomes all that is required by another merchant to accept a sale charge.

PayPal - Offers less protection to consumers than credit cards but provides privacy protection because consumer sensitive information is known only to PayPal.

Web sites and Portal Registrations –Offer consumers the convenience of using their email address as ID and using the same ID at many websites becomes a database key on different website and by linking information from these different web sites can lead to identity theft.

Internet Advertising – When a consumer clicks on an advertisement on the web portal and buy a product or printout a coupon and later use it the track number connect back to the ad on the particular website and thus the consumer has been profile and next time the consumer logs on the web site has an identity that leads to the consumer actual name.

Cookies- Is a file of data set by the web site and is stored on the consumer's computer. A cookie contains six fields (name, value, expiration date, path on the server to which it is to be delivered. A site can set many cookies (maximum of 4Kbytes). Some sites use cookies to provide customer with the convenience of not having to log on by storing user's ID and password!!! Cookies can also store credit card numbers, customer name and shipping address, last date site was visited, and detailed information on the financial transaction (items and price). Such information can be sold to third party.

Third party cookies- Can be found on web pages and belong to other organizations. Third party cookies can:

1. Count the frequency of a browser visiting a particular web page.
2. Track the pages viewed within one site
3. Count the number of advertisement has appeared on a page
4. Match a purchase with an advertisement view prior to purchase.
5. Record and report search strings from search engines

Privacy and Web Sites[191]

Smart Grid entities could consider using the standard set forth by The FTC and used by U.S. Web site.

The Federal Trade Commission (FTC) is the government entity with jurisdictions over both government and private web sites that solicit private user information. Since government web sites are covered under the Private Act FTC requires them to conform to privacy protection. The FTC concluded that for the U.S. government web sites to comply with the Privacy Act they must adheres to the following factors:

1. Notice: Data collecting entities must disclose their information practices to consumers before collecting consumers PII.
2. Choice: Data collecting entities must provide consumers with the choice of whether and how their collected PII may be used.
3. Access: Consumers must be provided with a process to view and contest the accuracy of their collected PII.
4. Security: Data collecting entities must have in place reasonable mechanisms to ensure that consumer collected PII is both accurate and secure from unauthorized use.
5. Enforcement: An enforceable mechanism to impose sanctions for noncompliance with these fair information practices.

Data Protection and Role Collaboration within Organizations

It is recommended for Smart Grid entities to develop a proactive and strategic approach that promotes collaboration among information security, privacy, business within their business see Appendix D

5.4 Research Topic in Implementing Privacy for Smart Grid

Laws and Regulations

U.S. government had established privacy laws that covers personal data collected and held by the U.S. government as well as specific data type collected by various organizations (See Appendix D). With several laws governing different data types two types of problems can occur. One is overlapping in which case which law would apply, the other is; what if there is a new data category (as maybe the case with Smart Grid) where there is now law on the books that covers this new derived data type. Analysis of the new derived data types in Smart Grid must be analyzed to highlight the need of new laws and regulation or perhaps the amendment of existing laws to include Smart Grid data.

Smart Grid data may be generated in one state and stored or queried by a Smart Grid entity in a different state and stored in yet a third state or even a different country. It is a legitimate question and research topic as to whether there is a need to have a law that governs Smart Grid

[191] FTC00, FTC. "Consumer Fraud and Identity Theft Complaint Data Jan-Dec 2005", white paper, 2006

data and not state level regulations? Or can Security policies established fail safe mechanisms to preserve subject data privacy? Case in point the California Breach law (SB1386) a scenario of such law violation is a non-California Smart Grid entity breached the privacy of a California resident but that entity resides in a state that has no such law.

Data collected by Smart Grid entities can violate trade secrets by analyzing the energy usage of a given company and therefore must be analyzed so consumer's privacy rights are not violated.

What constitute as Personal Identifiable Information can potentially cause loss of privacy once more for either the absence of a definition or differently defined definitions among Smart Grid entities.

Data Anonymization

Anonymity is one of method to preserve privacy. Use of multiple identities linked or not, pseudonymity in particular to protect against identity theft and for authentication. Analysis of Smart Grid use case data to determine how to effectively accomplish anonymity of consumers.

Privacy on the Web

Smart Grid consumer data should be protected and therefore all Smart entities that provide consumer with web access to their information or accounts should have the privacy as the default and not share consumer data without prior consumer consent. In the event of a privacy breach the consumer must be notified according to the established privacy policies.

Email Security

Despite the fact that email conceptually is a point to point communication it can potentially be exposed in a routing server and it has the potential interception risks similar to any web traffic. Entities providing consumers with email notification need to implement mechanisms to ensure consumer PI is not compromised.

Data Minimization

Entities involved in Smart Grid should utilize the use cases to determine the minimum consumer data required to perform the given task.

Privacy-Preserving Data Mining

Data Mining is the process of sifting through multiple databases and correlating data elements to find useful information. There are two approaches to data Mining correlation and aggregation. Generally speaking data mining threatens privacy as was proven by Sweeny identification is possible even when the identifying information is removed from a database.

Smart Grid can cause grave violation to individual privacy.

Privacy for Inference

Inferencing is a mechanism of driving sensitive data from non-sensitive data which can potentially affect privacy. The design of the DBMS allowable queries should forbid such

queries that can result in revealing sensitive information. Suppression and concealing are two techniques suggested by Denning and Schlorer for database security from inference attacks. Using suppression queries that result in sensitive data are rejected and concealing the result of the query is close to but not exact.

Privacy for Aggregation

Aggregation is a challenging problem due to the fact it can occur without violating either the DBMS or the security policy. Aggregation can potentially build sensitive results from less sensitive data (input) and therefore can indirectly affect privacy. One approach, Data Perturbation, can be used to preserve privacy. Data Perturbation by adding a positive or negative number to each data value as suggested by Agrawal and Srikant prove that it is possible to determine the distribution of the original data given both the distribution of the data after perturbation and that of the errors.

Privacy for Correlation

Correlation means joining databases on common attributes (fields). Such linkage of databases tables can compromise privacy. By controlling such linkage we can preserve privacy. Data Perturbation by swapping data fields was suggested by Vaidya and Clifton.

Data Encryption

Data encryption as a means of preserving privacy whether in storing data in databases, transmission of PI over the internet, use with third party entities for consumer access of energy usage or receiving of email notification regarding service as well as a mechanism in data anonymization and aggregation.

5.5 Conclusion

With the deployment of Smart meter technology consumers' daily life activities can potentially be reconstructed revealing sensitive information about people behavior and habits giving rise to privacy concerns due to fine granularity of the data collected. Thus the privacy concerns posed by Smart Meter data compel balancing exposure risks and public policies.

The privacy issues posed by the smart meter data is complex and challenging at best and must be addressed on two fronts.

First, regulatory measures need to be in place to ensure that standards and procedures are established and implemented to guard against the possibilities of a systematic misuse of consumers' information by the utilities or any third party involved with Smart Grid consumer information by ensuring that data is collected for the intended principle purpose only. Existing privacy laws and regulations might need to be amended to ensure that Smart Meter new types of data are addressed or new laws and regulations may be needed.

Second, technical measures must address both the security of the database of consumers' aggregated data stored by the utilities and the security of data transmission. The issues associated with security of data transmission are the same cyber security issues related to any

data transmission and database storage and access. The new challenges with Smart Meter data are the issues of

1. “Anonymization” of consumers’ aggregated data and the disposal of consumers’ information at the end of its usage duration. The failure to the ”anonymization” of data incidents recently with both Netflix and AOL points to the complexity of this issue.
2. Email security for example for consumer notification of power restoration services.
3. Privacy on the web for example for consumers accessing their account information.

The vision of creating an efficient and environmentally friendly electric grid hinges on consumers’ confidence in Smart Grid entities. This can be achieved when transparent privacy practices are implemented and enforced within Smart Grid.

CHAPTER 6:
Conclusion

As is indicated in the report, there are a number of potentially significant cyber security issues in the Smart Grid that should be addressed. Areas of vulnerabilities include confidentiality of user information, integrity of demand response systems, integrity and availability of SCADA (grid) systems, and integrity and availability of Plug-in Electric Vehicles. Furthermore, the researchers identified cyber security issues of communication systems in major components of the smart grid system, such as eavesdropping and Man-in-the-Middle attacks (MITM) in Advanced Metering Infrastructure (AMI), and also addressed various security threats/issues in communication protocols, such as acknowledgement forgery in Zigbee and MAC spoofing in IEEE 802.11. Additionally, constraints of devices, such as limitations in memory and short battery life of devices, which could introduce another security issue, were specified. Some of the issues are addressed in the Research and Development (R&D) topics specified in this report.

Because the smart grid will have extensive information systems component, the best practices and security mechanisms used on those systems can be applied to address those vulnerabilities. The uses of cryptography for technically handling security issues in major components of the smart grid systems were introduced. Although, in some cases (e.g. security policy creation), the best practices can be applied directly, there are other situations (e.g. firmware updates) where they cannot be used directly. Additionally, because of the unique characteristics of Smart Grid especially as a critical infrastructure, there are situations (e.g. intrusion detection), where further research will be needed to address security issues in those unique cases.

The researchers identified a number of areas that needed research including patch management, cost-effective tamper-resistant meters, cryptographic key management, wireless sensor networks, etc. The researchers found that with the exception of a few cases the processes and results of the research should be non-confidential.

As is indicated in the report, the privacy issues in the Smart Grid are also addressed. The researchers summarized the data flow and interfaces of the data to consumers, characteristics of smart meter data and the risks of data disclosure. The researchers emphasized the lack of consistency in privacy policies and addressed a number of privacy concerns in the Smart Grid. The concepts of Privacy by Design called SmartPrivacy, developed by Ann Cavoukian, were summarized in this report. Also, the privacy best practices addressed in this document include NIST recommendations for mitigating privacy concerns, data access risk elimination, privacy on the web, etc. Potential R&D issues for privacy in the Smart Grid were also identified as well. The results show that privacy issues posed by smart meter data are challenging and more research in privacy use cases and policies are needed in to help increase customers' confidence.

GLOSSARY

ACL	Access Control List
ACM	Association for Computing Machinery (ACM)
AES-CTR	Advanced Encryption Standard – Counter Mode
AMI	Advanced Metering Infrastructure
AMR	Automated Meter Reading
ASIS	American Society for Industrial Security
Auto-DR	Automated Demand Response
BMS	Building Management System
BPL	Broadband over Power Line
CCSS	Center for Control System Security
CEC	California Energy Commission
CHP	Combined Heat and Power
C&I	Commercial and Industrial
CIA	Central Intelligence Agency
CMMS	Computer Maintenance Management System
CSO	Chief Security Officer
DA	Distribution Automation
DER	Distributed Energy Resources
DFC	Dynamic Flow Concept
DHS	US Department of Homeland Security
DLC	Direct Load Control
DNP	Distributed Network Protocol
DoE	US Department of Energy
DOS	Denial of Service
DR	Demand-Response
DRAS	Demand Response Automation Server
DRRC	Demand Response Research Center

DSPF	Distribution System Power Flow
DSM	Demand Side Management
DSSS	Direct Sequence Spread Spectrum
EEI	Edison Electric Institute
EM	Electro-Magnetic
EMS	Energy Management System
EMCS	Emergency Management Control System
EPRI	Electric Power Research Institute
HAN	Home Area Network
HG	Home Gateway
HVAC	Heating Ventilation & Air Condition
HTTP	Hyper Transfer Text Protocol
ICCP	Inter-Control center Communications Protocol
ICS	Industrial Control Systems
IDART	Information Design Assurance Red Team
IED	Intelligent Electronic Devices
IOU	Investor Owned Utility
IP	Internet Protocol
ISO	Independent System Operator
IT	Information Technology
ITPS	Integrated Transportation Payment Systems
kW	Kilowatt
kWh	Kilowatt Hour
LAN	Local Area Network
LOS	Line of Sight
LSE	Load Serving Entity
LTC	Load Tap Changer
MAC	Media Access Control

MDM	Meter Data Management
MDMS	Meter Data Management System
MTU	Master Terminal Unit
NAN	Neighborhood Area Network
NIST	National Institute of Standards and Technology
NOC	Network Operating Center
OSCP	Online Certificate Status Protocol
OpenADR	Open Automated Demand Response or Open Auto-DR
PCT	Programmable Communicating Thermostat
PEV	Plug In Electric Vehicle
PG&E	Pacific Gas & Electric
PHEV	Plug In Hybrid Electric Vehicle
PIER	Public Interest Energy Research
PKI	Public Key Infrastructure
PLC	Programmable Logic Controllers
RCD	Residual Current Device
RD&D	Research, Development and Demonstration
RF	Radio Frequency
RFB	Request For Bids
RG	Residential Gateway
RTO	Regional Transmission Operators
RTP	Real Time Pricing
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SCE	Southern California Edison
SDLC	Systems Development Life Cycle
SG	Smart Grid
SOAP	Simple Object Access Protocol

T&D	Transmission and Distribution
TDM	Time Division Multiplexing
TLS	Transport Layer Security
TOU	Time to Use
UIS	Utility Information System
USNAP	Utility Smart Network Access Port
V2G	Vehicle to Grid
WNAN	Wireless Neighborhood Area Network
Wi-Max	Worldwide Interoperability for Microwave Access
WSDL	Web Service Description Language
XML	Extensible Markup Language
XSD	XML Schema Definition

REFERENCES

Cisco Smart Grid, Solutions for the next Generation Energy Network: http://www.cisco.com/web/strategy/docs/energy/aag_c45_539956.pdf

Ali Nourai, "Spyware". Smart Grid News. http://www.smartgridnews.com/artman/publish/News_Blogs_News/Foreign_ Cyber-Spies _Inject _Spyware_ into_U_S_Grid_with_Potential_for_Serious_Damage-562.html

Alex Yu Zheng, "Smart Security for Smart Grid: New Threats on the Horizon". Smart Grid News. http://www.smartgridnews.com/artman/publish/Technologies_Security_News/Smart-Security-for-a-Smart-Grid-New-Threats-on-the-Horizon-1226.html

Jeanne Meserve, "Smart Grid may be Vulnerable to Hackers". CNN. http://www.cnn.com/2009/TECH/03/20/smartgrid.vulnerability/index.html

Jude Clemente, "The Security Vulnerabilities of Smart Grid". Journal of Energy Security, June 2009. http://www.ensec.org/index.php?option=com_content&view=article&id=198: the-security-vulnerabilities-of-smart-grid&catid=96:content&Itemid=345

Infoworld, "Smart Grid Vulnerabilities Could Cause Widespread Disruptions". October 2009. http://cacm.acm.org/news/43974-smart-grid-vulnerabilities-could-cause-widespread-disruptions/fulltext

Timothy, "Smart Grid Computers Susceptible to Worm Attack". Slashdot, March 2009. http://hardware.slashdot.org/article.pl?sid=09/03/22/082236

Yao Liu, Peng Ning, Michael K. Reiter. False Data Injection Attacks against State Estimation in Electric Power Grids. Department of Computer Science, North Carolina State University. ftp://ftp.csc.ncsu.edu/pub/tech/2009/TR-2009-5.pdf

Roberto, http://www.cyberpunkreview.com/news-as-cyberpunk/the-cias-latest-claim-hackers-have-attacked-foreign-utilities/ Cyber Punk News, January 2008.

Shane Harris. http://www.nationaljournal.com/njmagazine/cs_20080531_6948.php National Journal Magazine, May 2008.

Charles E. Noble. http://www.nerc.com/docs/standards/Chuck-Noble-RBB-Letter.pdf CISSP Information Security, ISO New England.

Ali Nourai. "Foreign Cyber-Spies Inject Spyware into US Grid." http://www.smartgridnews.com/artman/publish/News_Blogs_News/Foreign_ Cyber-Spies _Inject _Spyware_ into_U_S_Grid_with_Potential_for_Serious_Damage-562.html. Smart Grid News.

Charles E. Noble. http://www.nerc.com/docs/standards/Chuck-Noble-RBB-Letter.pdf CISSP Information Security, ISO New England.

Wikipedia; Advanced Metering Infrastructure; Available [Online]: http://en.wikipedia.org/wiki/Advanced_Metering_Infrastructure

California Energy Commission's Public Interest Energy Research Program, PIER Buildings Program, *Automated Demand Response Cuts Commercial Building Energy Use and Peak*

Demand, Technical Brief, Public Interest Energy Research Program ,2008[online]. Available: http://www.energy.ca.gov/2008publications/CEC-500-2008-086/CEC-500-2008-086-FS.PDF

U.S. Federal Energy Regulatory Commission (FERC), *Assessment of Demand Response and Advanced Metering*, 2007[online]. Available: http://www.ferc.gov/legal/staff - reports/09 - 07 - demand - response.pdf

S. Kiliccote, M.A. Piette, J.H. Dudley, Lawrence Berkeley National Laboratory (LBNL); E. Koch and D. Hennage, Akuacom, *Open Automated Demand Response for Small Commercial Buildings*, Lawrence Berkeley National Laboratory ,July 2009 [online]. Available: http://drrc.lbl.gov/pubs/lbnl-2195e.pdf

M.A. Piette, G. Ghatikar, S. Kiliccote, E. Koch, D. Hennage, P. Palensky, and C. McParland, *Open Automated Demand Response Communications Specification*, Demand Response Research Center, April 2009 [online]. Available: http://drrc.lbl.gov/openadr/pdf/cec-500-2009-063.pdf

E. Koch, Akuacom; M.A. Piette, Lawrence Berkeley National Laboratory (LBNL), *Architecture Concepts and Technical Issues for an Open, Interoperable Automate Demand Response Infrastructure*, 2007 [online]. Available: http://www.gridwiseac.org/pdfs/forum_papers/104_paper_final.pdf

Lee, T. Brewer, Computer Security Division, Information Technology Laboratory, National Institution of Standards and Technology (NIST), *Smart Grid Cyber Strategy and Requirements*, Draft NISTIR 7628, Sept 2009 [online]. Available: http://csrc.nist.gov/publications/drafts/nistir-7628/draft-nistir-7628.pdf

K. Stouffer, J. Falco, K. Scarfone, *Guide to Industrial Control Systems (ICS) Security*, National Institution of Standards and Technology (NIST), Sept 2008 [online]. Available: http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf

E. W. Gunther, *Reference Design for Programmable Communicating Thermostats Compliant with Title 24-2008* , March 2007 [online]. Available: http://drrc.lbl.gov/pct/docs/ReferenceDesignTitle24PC_rev15.doc

R. Ramesh, *CSCTG Demand Response Interfaces NISTIR*, Aug 2008 [online]. Available: http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CsCTGDR/CSCTG-DR-Draft_082809.doc

Khusvinder Gill, Shuang-Hua Yang, Fang Yao, and Xin Lu *A ZigBee-Based Home Automation System*. Loughborough University, UK 2009.

http://www.usnap.org/technical.aspx

Matera: *Security Issues on ZigBee* Basilicata University, Italy, January 18, 2006

Ken Masica, *Recommended Practices Guide For Securing ZigBee Wireless Networks in Process Control System Environments,* Lawrence Livermore National Laboratory

M.A. Piette, G. Ghatikar, S. Kiliccote, E. Koch, D. Hennage, P. Palensky, and C. McParland, "Open Automated Demand Response Communications Specification", Demand

Response Research Center, April 2009 [online]. Available: http://drrc.lbl.gov/openadr/pdf/cec-500-2009-063.pdf. [Accessed October 20, 2009]

E. W. Gunther, "Reference Design for Programmable Communicating Thermostats Compliant with Title 24-2008", March 2007 [online]. Available: http://drrc.lbl.gov/pct/docs/ReferenceDesignTitle24PC_rev15.doc. [Accessed October 22, 2009]

K. Stouffer, J. Falco, K. Scarfone, Guide to Industrial Control Systems (ICS) Security, National Institution of Standards and Technology (NIST), Sept 2008 [online]. Available: http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf

A. Lee, T. Brewer, Computer Security Division, Information Technology Laboratory, National Institution of Standards and Technology (NIST), Smart Grid Cyber Strategy and Requirements, Draft NISTIR 7628, Sept 2009 [online]. Available: http://csrc.nist.gov/publications/drafts/nistir-7628/draft-nistir-7628.pdf

E. W. Gunther, Reference Design for Programmable Communicating Thermostats Compliant with Title 24-2008 March 2007 [online]. Available: http://drrc.lbl.gov/pct/docs/ReferenceDesignTitle24PC_rev15.doc

Bob Fleck, Bruce Potter. *802.11 Security*. O'Reilly Publications, December 2002, ISBN : 0-596-00290-4

Naveen Shastry, David Wagner, *Security Considerations for IEEE 802.15.4 Networks*. UC Berkley. Year of Publication – 2004.

Keith Stouffer Joe Falco, Karen Scarfone .*Guide to Industrial Control Systems (ICS) Security* (Special Publication 800-82 FINAL PUBLIC DRAFT). National Institute of Standards and Technology, US department of Commerce.

East, Samuel. Butts, Jonathan. Papa, Mauricio. And Shenoi, Sujeet. *A taxonomy of attacks on the DNP3 Protocol*. Critical Infrastructure Protection III, IFIP AICT 311, pp. 67–81, 2009. IFIP International Federation for Information Processing (2009).

Robert F. Dacey, Director, Information Security Issues. *Critical Infrastructure Protection, Challenges in Securing Control*. US Government Accountability Office, United States General Accounting Office October 2003.

Chikuni, Edward and Dondo, Maxwell. *Investigating the security of Electrical Power Systems SCADA*. (2007).

Paar, Christof, Andy Rupp, Kai Schramm, Andre Weimerskirch, and Wayne Burleson. *Securing Green Cars: IT Security in Next-Generation Electric Vehicle Systems.* Tech. Amherst: ECE Department, University of Massachusetts at Amherst. Print [PEV-2] Vehicle-to-grid. *Vehicle-to-grid* -Wikipedia, the free encyclopedia. Wikipedia, 2 Oct. 2009.

Microsoft Developer Network (MSDN) library, Microsoft Corporation, "Web Service Security Scenarios, Patterns, and Implementation Guidance for Web Services Enhancements (WSE) 3.0", 2009 [online]. Available: http://msdn.microsoft.com/en-us/library/aa480545.aspx. [Accessed Dec 4, 2009]

W. Stalling, L. Brown , "Computer Security Principles and Practice: Chapter 2 – Cryptographic Tools", First Edition, 2008 [online]. Available: http://people.eecs.ku.edu/~saiedian/Teaching/Fa09/710/Lectures/ch02.pdf. [Accessed Jan 20, 2010]

National Institute of Standard and Technology (NIST), "Digital Signature Standard (FIPS 186-3)", June 2009 [online]. Available: http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf. [Accessed Jan 20, 2010]

Smart Grid Security: Vulnerabilities from Carbon-Pros Analyst Blog, August 24, 2009 Available (Online): http://carbon-ros.com/blog1/2009/08/smart_grid_security_vulnerabil.html

Advanced Metering Infrastructure Security Considerations by Raymond C. Parks. http://www.oe.energy.gov/DocumentsandMedia/20-AMI_Security_Considerations.pdf

Smart Security for a Smart Grid: New Threats on the Horizon – Smart Grid News.com – By Alex Yu Zheng. Posted On: Sep 28, 2009. http://www.smartgridnews.com/artman/publish/industry/Data_Privacy_and_Security_Issues_for_Advanced_Metering_Systems_Part_2-453.html

Tamper-resistant smart power meters rely on isolated sensors by Margery Conner, posted on March 19, 2009. Available (Online): http://www.edn.com/article/CA6643364.html

Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures by Chris Karlof and David Wagner. http://webs.cs.berkeley.edu/papers/sensor-route-security.pdf

Smart Grid: New Views on Countermeasures by Jack Danahy. Posted on December 7, 2009. http://smartgridsecurity.blogspot.com/2009/12/smart-grid-new-views-on-countermeasures.html

'Smart Grid' may be vulnerable to hackers – CNN.com – By Jeanne Meserve. Posted On: Mar 21, 2009. http://www.cnn.com/2009/TECH/03/20/smartgrid.vulnerability/index.html

Smart Grid Computers Susceptible To Worm Attack – By Timothy. Posted On: Mar 22, 2009 http://hardware.slashdot.org/article.pl?sid=09/03/22/082236

The Security Vulnerabilities of Smart Grid - By Jude Clemente, Journal of Energy Security. Posted On: Jun 18, 2009 http://www.ensec.org/index.php?option=com_content&view=article&id=198:the-security-vulnerabilities-of-smart-grid&catid=96:content&Itemid=345

Critical Infrastructure Protection for AMI Using a Comprehensive Security Platform. Posted on February 2009 http://osgug.ucaiug.org/utilisec/amisec/Shared%20Documents/Forms/AllItems.aspx?RootFolder=%2futilisec%2famisec%2fShared%20Documents%2f0.%20AMI%20Risk%20Assessment&FolderCTID=&View={7B63C81F-617F-4FC1-AFCB-8404B6B6B0A7}

REQUEST TO APPROVE PROPOSED CYBER SECURITY STANDARD – By Charles E. Noble http://www.nerc.com/docs/standards/Chuck-Noble-RBB-Letter.pdf

Microsoft Statement on the "Slammer" Worm Attack by Wash Redmond. Posted on January 28, 2003
http://www.microsoft.com/presspass/press/2003/jan03/01-25virus.mspx

False Data Injection Attacks against State Estimation in Electric Power Grids – By Yao Liu, Peng Ning and Michael K. Reiter
ftp://ftp.csc.ncsu.edu/pub/tech/2009/TR-2009-5.pdf

An Interleaved Hop-by-Hop Authentication Scheme for Filtering of Injected False Data in Sensor Networks by Sencun Zhu, Sanjeev Setia, Sushil Jajodia and Peng Ning.
http://www.cse.psu.edu/~szhu/papers/tinymesh.pdf

Wikipedia; Advanced Metering Infrastructure;
http://en.wikipedia.org/wiki/Advanced_Metering_Infrastructure

Open Smart Grid; Shared Documents;
http://osgug.ucaiug.org/Shared%20Documents/Forms/AllItems.aspx

Microsoft Developer Network (MSDN) library, Microsoft Corporation, "Web Service Security Scenarios, Patterns, and Implementation Guidance for Web Services Enhancements (WSE) 3.0", 2009 [online]. Available: http://msdn.microsoft.com/en-us/library/aa480545.aspx. [Accessed Dec 4, 2009]

W. Stalling, L. Brown , "Computer Security Principles and Practice: Chapter 2 – Cryptographic Tools", First Edition, 2008 [online]. Available: http://people.eecs.ku.edu/~saiedian/Teaching/Fa09/710/Lectures/ch02.pdf. [Accessed Jan 20, 2010]

National Institute of Standard and Technology (NIST), "Digital Signature Standard (FIPS 186-3)", June 2009 [online]. Available: http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf. [Accessed Jan 20, 2010]

D. K. Mulligan, D. Wagner, U. Shankar, P.A. Subrahmanyam, E. Jones, J. Lerner. "Network Security Architecture for Demand Response/Sensor Networks". Technical report, On behalf of California Energy Commission, Public Interest Energy Research Group, January, 2005 [online]. Available: http://www.law.berkeley.edu/files/demand_response_CEC.pdf. [Accessed Nov 30, 2009]
http://technet.microsoft.com/en-us/library/bb457091.aspx

Wikipedia: IEEE 802.11 http://en.wikipedia.org/wiki/IEEE_802.11w-2009

Ken Masica, Recommended Practices Guide for Securing Zigbee Wireless Networks in Process Control System Environments. Draft version. Lawrence Livermore National Laboratory. April 2007.

Hyung-Joon Kim, IEEE 802.16/WiMax Security, Stevens Institute of Technology, Hoboken, New Jersey

P Kitsos, O Koufopavlou, G Selimis and N Sklavos , Low Power Cryptography, VLSI Design Lab, Electrical and Computer Engineering Department, University of Patras.

Khusvinder Gill, Shuang-Hua Yang, Fang Yao, and Xin Lu A ZigBee-Based Home Automation System. Loughborough University, UK 2009.

Ken Masica, Recommended Practices Guide for Securing Zigbee Wireless Networks in Process Control System Environments. Draft version. Lawrence Livermore National Laboratory. April 2007.

D. K. Mulligan, D. Wagner, U. Shankar, P.A. Subrahmanyam, E. Jones, J. Lerner. "Network Security Architecture for Demand Response/Sensor Networks". Technical report, On behalf of California Energy Commission, Public Interest Energy Research Group, January, 2005:
http://www.law.berkeley.edu/files/demand_response_CEC.pdf.

M.J.B. Robshaw, Y. L. Yin, "Overview of Elliptic Curve Cryptosystems", RSA Laboratories Technical Note, June 1997.
http://www.rsa.com/rsalabs/node.asp?id=2013

B. Kaliski, "*TWIRL and RSA Key Size*", RSA Laboratories Technical Note, May 2003 http://www.rsa.com/rsalabs/node.asp?id=2004.

S. Wander; University of California at Santa Cruz, N. Gura, H. Eberle, V. Gupta, Sheueling C. Shantz; Sun Microsystems Laboratories "Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks", March 2005 http://research.sun.com/projects/crypto/wandera_energyanalysis.pdf.

V. Gupta, S. Gupta, S. Chang; Sun Microsystems Inc. "Performance Analysis of Elliptic Curve Cryptography for SSL", 2002 [online]. Available: http://research.sun.com/projects/crypto/performance.pdf. [Accessed Jan 20, 2010]

Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS) http://tools.ietf.org/html/rfc4492

K. Masica; Lawrence Livermore National Laboratory, Recommended Practices Guide For Securing ZigBee Wireless Networks in Process Control System Environments (Draft), April 2007 http://csrp.inl.gov/Documents/Securing%20ZigBee%20Wireless%20Networks%20in%20Process%20Control%20System%20Environments.pdf

Federal Information Processing Standards Publication 197"Advance Encryption Standard (AES)", Nov 2001: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

B. Gohn; Ember Cooperation, "Smart Meters and Home Automation", May 2008: http://www.pointview.com/data/2008/05/22/pdf/Bob-Gohn-3024.pdf.

R. Cragie, "Public Key Cryptographic in Zigbee Network", Dec 2008. http://www.elektroniknet.de/fileadmin/user_upload/pdf/euzdc2008/Cragie_Jennic.pdf

Josh Wright; InGuardian, "an attack framework designed to explore vulnerabilities in ZigBee and wireless sensor networks." Oct 2009.

http://inguardians.com/pubs/toorcon11-wright.pdf.

E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid; National Institute of Standard and Technology (NIST), "Recommendation for Key Management – Part 1: General (Revised)", SP800-57, Mar 2008 http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf.

M.A. Piette, G. Ghatikar, S. Kiliccote, E. Koch, D. Hennage, P. Palensky, and C. McParland, "Open Automated Demand Response Communications Specification", Demand Response Research Center, April 2009
http://drrc.lbl.gov/openadr/pdf/cec-500-2009-063.pdf.

B. Kaliski, *"TWIRL and RSA Key Size"*, RSA Laboratories Technical Note, May 2003. http://www.rsa.com/rsalabs/node.asp?id=2004.

M. Ray, S. Dispensa, PhoneFactor, Inc., "Renegotiation TLS version 1.1", Nov 4, 2009. http://extendedsubset.com/?p=8.

Microsoft Developer Network (MSDN) library, Microsoft Corporation, "Web Service Security Scenarios, Patterns, and Implementation Guidance for Web Services Enhancements (WSE) 3.0", 2009. http://msdn.microsoft.com/en-us/library/aa480545.aspx.

Digital Signature Standard: http://www.itl.nist.gov/fipspubs/fip186.htm

Wikipedia, "Digital Signature", Nov 2009 : http://en.wikipedia.org/wiki/Digital_signature

Nadalin, IBM Corporation; C. Kaler, Microsoft Corporation; P. Hallam-Baker, VeriSign Inc.; R. Monzillo, Sun Microsystems Inc., "Web Services Security: SOAP Message Security 1.0 (WS-Security2004) OASIS Standard 200401", March 2004
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf.

E. W. Gunther, "Reference Design for Programmable Communicating Thermostats Compliant with Title 24-2008", March 2007
http://drrc.lbl.gov/pct/docs/ReferenceDesignTitle24PC_rev15.doc

Pserc_smart_grid_white_paper_march_2009_adobe7.pdf; http://www.pserc.wisc.edu/ecow/get/publicatio/2009public/pserc_smart_grid_white_paper_march_2009_adobe7.pdf

Robert F. Dacey, Director, Information Security Issues Oct 2003, "CRITICAL INFRASTRUCTURE PROTECTION, Challenges in Securing Control Systems". http://www.gao.gov/new.items/d04140t.pdf

Edward Chikuni, Department of Electrical Engineering Polytechnic University of Namibia, Namibia, Maxwell Dondo, Defence R&D Ottawa, 2007 " Investigating the Security of Electrical Power Systems SCADA". http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4401531&tag=1

Micrologic System Inc, "SCADA primer", http://www.micrologic-systems.com/primers/scada.htm

Chee-Wooi Ten, Student Member, IEEE, Iowa State University, Manimaran Govindarasu, Member, IEEE, Iowa State University, and Chen-Ching Liu, Fellow, IEEE, Iowa State University 2007, "Cyber security for Electric Power Control and Automation Systems". http://powercyber.ece.iastate.edu/publications/SMC-conf.pdf

Dale Peterson, Director, Network Security Practice Digital Bond, Inc, "Intrusion Detection and Cyber Security Monitoring of SCADA and DCS Networks". http://www.isa.org/filestore/Division_TechPapers/GlassCeramics/TP04AUTOW046.pdf

Gordon Clarke, Deon Reynders, Edwin Wright, "Practical Modern SCADA Protocols:

DNP3, 60870.5 and Related Systems" British Library Cataloguing in Publication Data, ISBN 07506 7995. http://www.sensorsportal.com/HTML/BOOKSTORE/SCADA_Protocols.htm

Samuel East, Jonathan Butts, Mauricio Papa and Sujeet Shenoi, "A Taxonomy of attacks on the DNP3 protocol". http://www.springerlink.com/content/k48k4733v0367120

James H. Graham, Sandip C. Patel, Dept. of Computer Engineering and Computer Science. University of Louisville, September 2004, "*Security Considerations in SCADA Communication Protocols*". http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.84.1152

Munir Majdalawieh1, Francesco Parisi-Presicce, Duminda Wijesekera," *DNPSec: Distributed Network Protocol Version 3 (DNP3) Security Framework*". http://www.acsac.org/2005/techblitz/majdalawieh.pdf

Grant Gilchrist, PE, FnerNex Corporation, Okotoks, 2008," *Secure Authentication for DNP3*". http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4596147

Woody, Todd. *"PG&E's Battery Power Plans Could Jump Start Electric Car Market."* http://www.mthink.com/utilities/phevs-are-roll

it_security_for_electric_vehicles.pdf; Available online : http://www.crypto.ruhr-uni-bochum.de/imperia/md/content/texte/publications/conferences/it_security_for_electric_vehicles.pdf

http://www.edn.com/article/CA6643364.html

I. Ghansah, "Smart Grid Cyber Security Potential Threats, Vulnerabilities and Risk", California Energy Commission, PIER Energy-Related Environmental Research Program. CEC-500-2008-027, October 2009.

I. Ghansah, ”Best Practices for Handling Smart Grid Cyber Security“, California Energy Commission, PIER Energy-Related Environmental Research Program. CEC-500-2008-027, February 2010.

D. Andert, R. Wakefield, and J. Weise, Professional Service Security; Sun Microsystems Inc., “Trust Modeling for Security Architecture Development”, December 2002 [online]. Available: http://www.sun.com/blueprints/1202/817-0775.pdf

M. Blaze, J. Feigenbaum, and J. Ioannidis; AT&T Labs – Research, A. Keromytis; U. of Pennsylvania, “The KeyNote Trust-Management System Version 2”, September 1999 [online]. Available: http://www.cs.columbia.edu/~angelos/Papers/rfc2704.txt

M. Blaze, J. Feigenbaum, and J. Ioannidis; AT&T Labs – Research, A. Keromytis; U. of Pennsylvania, “The KeyNote Trust-Management System Version 2”, September 1999 [online]. Available: http://www.cs.columbia.edu/~angelos/Papers/rfc2704.txt

I. Ghansah; California State University Sacramento, D. Thanos; GE Digital Energy, P. Pal, and R. Schantz; BBN, C. Gunter, T. Yardley, and Himanshu Khurana; University of Illinois, E. Beroset; Elster, S. Klein; OSECS, R. Jepson; Lockheed Martin, J. Ascough, and R. Henning; Harris Corp. P. Blomgren; SafeNet, G. Emelko; ACLARA Tech, K Garrard; Aunigma Network Security Corp, “R&D Themes for Cyber Security in the Smart Grid”, March 25, 2010 [online]. Available: http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CSCTGRandD/RDIdeas-March30_2010.doc

A. Lee, T. Brewer; The Cyber Security Coordination Task Group, “DRAFT NISTIR 7628 - Smart Grid Cyber Security Strategy and Requirements”, September 2009 [online]. Available: http://csrc.nist.gov/publications/drafts/nistir-7628/draft-nistir-7628.pdf

M. Enstrom, “(DRAFT) Privacy Chapter Introduction”, April 06, 2010 [online]. Available: http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/NISTIR7628PrivacyIntroApr2010

A. Arsenault; Diversinet, S. Turner; IECA, PKIX Working Group, “Internet X.509 Public Key Infrastructure: Roadmap”, July 2002 [online]. Available: http://tools.ietf.org/html/draft-ietf-pkix-roadmap-09

National Institute of Standard and Technology (NIST), “Digital Signature Standard (FIPS 186-3)”, June 2009 [online]. Available: http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf.

E.Stavrou, “PKI: Looking at the Risks”, January 2005 [online]. Available: http://www.devshed.com/c/a/Security/PKI-Looking-at-the-Risks/

E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid; National Institution of Standard and Technologies (NIST), “Recommendation for Key Management – Part 1: General (revised)”, March 08, 2007 [online]. Available: http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf

G. Appenzeller, L. Martin; Voltage Security, M. Schertler; Tumbleweed Communications, "Identity-based Encryption Architecture", Internet Draft, November 2007 [online]. Available: http://tools.ietf.org/html/draft-ietf-smime-ibearch-06

M. Gagné, "Identity-Based Encryption: a Survey", RSA Laboratories Cryptobytes, Vol. 6, No. 1, Spring 2003

Identity based encryption, Russell Kay Computer world Nov 17th 2008

A White Paper by Vertoda, "An Overview of Identity Based Encryption", 2009 [online]. Available: http://www.slideshare.net/vertoda/an-overview-of-identity-based-encryption

G. Appenzeller; Stanford University, L. Martin; Voltage Security, M. Schertler; Axway, "Identity-based Encryption Architecture and Supporting Data Structure", January 2009 [online]. Available: http://tools.ietf.org/search/rfc5408

WikiPedia, "Trused Platform Module", April 2010 [online]. Available: http://en.wikipedia.org/wiki/Trusted_Platform_Module

WikiPedia, "Trused Platform Module", April 2010 [online]. Available: http://en.wikipedia.org/wiki/Trusted_Platform_Module

S. Bajikar; Mobile Platform Group, Intel Corporation, "Trusted Platform Module (TPM) based Security on Notebook PCs – White Paper", June 20, 2002 [online]. Available: http://www.intel.com/design/mobile/platform/downloads/Trusted_Platform_Module_White_Paper.pdf

TPM specification, version 1.2, Revision 103. http://www.trustedcomputinggroup.org/resources/tpm_main_specification

P. Kitsos, O. Koufopavalou, G. Selimis and N. Sklavos VlSI Design Lab, Electrical and computer dept, University of Patras Rio, 26500 Patras, Greece, "Low power cryptography", [online]. Available: http://iopscience.iop.org/1742-6596/10/1/084/pdf/jpconf5_10_084.pdf?ejredirect=migration

J. Fox, B. Gohn, C. Wheelock, "Networking and Communications, Energy Management, Grid Automation, and Advanced Metering Infrastructure", PIKERESEARCH , 4Q 2009.

K. Gill, S. Hua Yang, F. Yao, and X. Lu; IEEE Transactions on Consumer Electronics, "A ZigBee-Based Home Automation System", Vol. 55, No. 2, May 2009 [online]. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=05174403

E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid; National Institution of Standard and Technologies (NIST), "Recommendation for Key Management – Part 1: General (revised)", March 08, 2007 [online]. Available: http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf

R. Cragie, "Public Key Cryptographic in Zigbee Network", Dec 2008. [online]. Available: http://www.elektroniknet.de/fileadmin/user_upload/pdf/euzdc2008/Cragie_Jennic.pdf

A. Geriks, J. Purcell, "A Survey of Wireless Mesh Networking Security Technology and Threats", SANS Institute, September 2006.

I. Ghansah, "Smart Grid Cyber Security Potential Threats, Vulnerabilities and Risk", California Energy Commission, PIER Energy-Related Environmental Research Program. CEC-500-2008-027, October 2009.

N. Shastry, D. Wagner; UC Berkley., "Security Considerations for IEEE 802.15.4 Networks", Year of Publication – 2004.

Security in Computing by Charles P. Pfleeger and Shari Lawrence Pfleeger

Managing and Protecting Personal Information, A Microsoft Perspective on Data Governance for Privacy and Compliance for the Enterprise, February 2009

Privacy and the New Energy Infrastructure by Elias L. Quinn, Draft: February 2009 Smart Grid Privacy

Privacy and the Smart Grid, Chapter 2 of NIST Security Document

Privacy of Consumer Information and Devices in the Electric Power Industry prepared by the Grid Wise Architecture Council/NIST Home-to-Grid Domain Expert Working Group Smart

Privacy for the Smart Grid: Embedded Privacy into the Design of Electricity Conservation by: The Future of Privacy Forum, November 2009

Privacy by Design: The Future of Privacy Forum, November 2009

NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.o

http://www.naruc.org/Resolutions/privacy_principles.pdf

http://www.philly.com/inquirer/business/20090906_Utilities_smart_meters_save_money_but_erode_privacy.html

http://infotech.aicpa.org/Resources/Privacy/Generally+Accepted+Privacy++An+Introductions+to+Generally+Accepted+Privacy+Principles.htm

http://csrc.nist.gov/publicatons/PubsDrafts.html#NIST-IR-7628

www.nationmaster.com

www.eia.doe.goc

www.epa.gov

APPENDIX A:
Key Power System Use Cases and Cyber Security Requirements

The following Use Cases were obtained from the NISTIR 7628 Smart Grid Cyber Security Strategy and Requirements (Sept 2009) which presented a full set of Use Cases taken from many sources, including the following:

- IntelliGrid Use Cases, only the power system operations Use Cases and Demand Response/AMI ones are of particular interest for security. The EPRI IntelliGrid project developed the complete list of Use Cases (700 cases).
- AMI Business Functions which were extracted from Appendix B of the AMI-SEC Security Requirements Specification.
- Benefits and Challenges of Distribution Automation – Use Case Scenarios extracted from CEC document which has 82 Use Cases.
- EPRI Use Case Repository, compilation of IntelliGrid and SCE Use Cases, plus others.
- SCE Use Cases developed by Southern California Edison (SCE) with the assistance of EnerNex.

The Use Cases has been grouped in categories that follow and they represent a good summary of most of the information discussed in this report.

1.1. Category: AMI

Scenario 1: Meter Reading Services (Periodic Meter Reading, On-Demand Meter Reading,

Net Metering for DER and PEV, Feed-In Tariff Metering for DER and PEV, Bill - Paycheck Matching)

Cyber Security Requirements:

Integrity of meter data is important, but the impact of incorrect data is not large.

Availability of meter data is not critical in real-time.

Confidentiality (privacy) of customer metering data over the AMI system, metering database, and billing database, to avoid serious breaches of privacy and potential legal repercussions.

Scenario 2: Pre-Paid Metering (Limited Energy Usage and Limited Demand)

Cyber Security Requirements:

Integrity of meter data is critical, to avoid unwarranted disconnections due to perceived lack of pre-payment. Security compromises could have a large impact on the customer and could cause legal repercussions

Availability to turn meter back on after payment is important, but could be handled by a truck roll if necessary.

Confidentiality (privacy) of customer metering data over the AMI system, metering database, and billing database is important.

Scenario 3: Revenue Protection (Tamper Detection, Anomalous Readings, Meter Status and Suspicious Meter)

Cyber Security Requirements:

Integrity of meter data is important, but if tampering is not detected or if unwarranted indications of tampering are detected, there is no power system impact, just revenue impact

Availability to turn meter back on after payment is important.

Confidentiality (privacy) of customer metering data over the AMI system, metering database, and billing database is important.

Scenario 4: Remote Connect/Disconnect of Meter (Remote Connect for Move-In, Remote Connect for Reinstatement on Payment, Remote Disconnect for Move-Out, Remote Disconnect for Non-Payment, Remote Disconnect for Emergency Load Control and Unsolicited Connect / Disconnect Event)

Cyber Security Requirements:

Integrity of control commands to the RCD switch is critical to avoid unwarranted disconnections or dangerous/unsafe connections. The impact of invalid switching could be very large if many meters are involved.

Availability to turn meter back on when needed is important.

Confidentiality requirements of the RCD command is generally not very important, except related to non-payment.

Scenario 5: Outage Detection and Restoration (Smart meters report one or more power losses e.g. "last gasp", Outage management system collects meter outage reports and customer trouble calls, Outage management system determines location of outage and generates outage trouble tickets, Work management system schedules work crews to resolve outage, Interactive utility-customer systems inform the customers about the progress of events and Trouble tickets are used for statistical analysis of outages)

Cyber Security Requirements:

Integrity is important to ensure outages are reported correctly.

Availability is important to ensure outages are reported in a timely manner (a few seconds).

Confidentiality is not very important.

Scenario 6: Meter Maintenance (Connectivity validation, Geo-location of meter and Smart meter battery management)

Cyber Security Requirements:

Integrity of meter maintenance repairs and updates are essential to prevent malicious intrusions.

Availability is important, but only in terms of hours or maybe days.

Confidentiality is not important unless some maintenance activity involves personal information.

Scenario 7: Meter Detect Removal

This scenario discusses the AMI meter's functionality to detect and report unauthorized removal and similar physical tampering. AMI meters require additional capability over traditional meters to prevent theft and tampering due to the elimination of regular visual inspection provided by meter reading.

Objective/ Requirements:

To reduce energy theft. To prevent theft/compromise of passwords and key material. To prevent installation of malware.

Scenario 8: Utilities detects Probable meter Bypass

AMI meters eliminate the possibility of some forms of theft (i.e. meter reversal). Other types of theft will be more difficult to detect due to the elimination of regular physical inspection provided by meter reading. This scenario discusses the analysis of meter data to discover potential theft occurrences.

Objective/ Requirements:

To reduce theft. To protect integrity of reporting. To maintain availability for reporting and billing

1.2. Category: Demand Response

Scenario 1: Real Time Pricing (RTP) for Customer Load and DER/PEV

Use of Real Time Pricing for electricity is common for very large customers, affording them an ability to determine when to use power and minimize the costs of energy for their business. The extension of real time pricing to smaller industrial and commercial customers and even residential customers is possible with smart metering and in-home displays. Aggregators or customer energy management systems must be used for these smaller consumers due to the complexity and 24x7 nature of managing power consumption. Pricing signals may be sent via an AMI system, the Internet, or other data channels.

Cyber Security Requirements:

Integrity, including non-repudiation, of pricing information is critical, since there could be large financial and possibly legal implications.

Availability, including non-repudiation, for pricing signals is critical because of the large financial and possibly legal implications.

Confidentiality is important mostly for the responses that any customer might make to the pricing signals.

Scenario 2: Time of Use (TOU) Pricing

Time of use pricing creates blocks of time and seasonal differences that allow smaller customers with less time to manage power consumption to gain some of the benefits of real time pricing. This is the favored regulatory method in most of the world for dealing with global warming

Although Real Time Pricing is more flexible than Time of Use, it is likely that TOU will still provide many customers with all of the benefits that they can profitably use or manage.

Cyber Security Requirements:

Integrity is not critical since TOU pricing is fixed for long periods and is not generally transmitted electronically.

Availability is not an issue.

Confidentiality is not an issue, except with respect to meter reading.

Scenario 3: Net Metering for DER and PEV

When customers have the ability to generate or store power as well as consume power, net metering is installed to measure not only the flow of power in each direction, but also when the net power flows occurred. Often Time of Use (TOU) tariffs are employed.

Today larger C&I customers and an increasing number of residential and smaller C&I customers have net metering installed for their photovoltaic systems, wind turbines, combined heat and power (CHP), and other DER devices. As plug-in electric vehicles (PEVs) become available, net metering will increasingly be implemented in homes and small businesses, even parking lots.

Cyber Security Requirements:

Integrity is not very critical since net metering pricing is fixed for long periods and is not generally transmitted electronically.

Availability is not an issue.

Confidentiality is not an issue, except with respect to meter reading.

Scenario 4: Feed-In Tariff Pricing for DER and PEV

Feed-in tariff pricing is similar to net metering except that generation from customer DER/PEV has a different tariff rate than the customer load tariff rate during specific time periods.

Cyber Security Requirements:

Integrity is not critical, since feed-in tariff pricing is fixed for long periods and is generally not transmitted electronically.

Availability is not an issue.

Confidentiality is not an issue, except with respect to meter reading.

Scenario 5: Critical Peak Pricing

Critical Peak Pricing builds on Time of Use Pricing by selecting a small number of days each year where the electric delivery system will be heavily stressed and increasing the peak (and sometime shoulder peak) prices by up to 10 times the normal peak price. This is intended to reduce the stress on the system during these days.

Cyber Security Requirements:

Integrity is not critical, since feed-in tariff pricing is fixed for long periods and is generally not transmitted electronically.

Availability is not an issue.

Confidentiality is not an issue, except with respect to meter reading.

Scenario 6: Mobile Plug-In Electric Vehicle (PEV) Functions

Customer connects PEV at another home. Customer connects PEV outside home territory.

Customer connects PEV at public location. Customer charges the PEV.

Cyber Security Requirements:

Integrity is not critical, since feed-in tariff pricing is fixed for long periods and is generally not transmitted electronically.

Availability is not an issue.

Confidentiality is not an issue, except with respect to meter reading.

1.3. Category: Customer Interfaces

Scenario 1: Customer's In Home Device is Provisioned to Communicate With the Utility

The process to configure a customer's device to receive and send data to utility systems. The device could be an information display, communicating thermostat, load control device or smart appliance.

Objective/Requirements:

To protect passwords. To protect key material. To authenticate with other devices on the AMI system.

Scenario 2: Customer Views Pricing or Energy Data on Their In Home Device

The information that should be available to customers on their in home devices.

Multiple communication paths and device functions will be considered.

Objective/Requirements:

To validate that information is trustworthy (integrity).

Scenario 3: In Home Device Troubleshooting

The resolution of communication or other types of errors that could occur within home devices. Roles of the customer, device vendor and utility will be discussed.

Objective/Requirements:

To avoid disclosing customer information, key material and/or passwords.

Scenario 4: Customer Views Pricing or Energy Data via the Internet

The information that should be available to the customer using the internet and some possible uses for the data.

Objective/Requirements:

Protect customer's information (privacy). Provide accurate information.

Scenario 5: Utility Notifies Customers of Outage

When an outage occurs the utility can notify affected customers and provide estimated restoration times and report when power has been restored. Smart grid technologies can improve the utility's accuracy for determination of affected area and restoration progress.

Objective/Requirements:

Validate that the notification is legitimate. Customer's information is kept private.

Scenario 6: Customer Access to Energy-Related Information

Access to real-time (or near real-time) energy and demand usage and billing information.

Requesting energy services such as move-in/move-out requests, pre-paying for electricity, changing energy plans (if such tariffs become available), etc.

Access to energy pricing information.

Access to their own DER generation/storage status.

Access to their own PEV charging/discharging status.

Establishing thermostat settings for demand response pricing levels.

Although different types of energy-related information access is involved, the security requirements are similar.

Cyber Security Requirements:

Integrity, including non-repudiation, is critical since energy and pricing data will have financial impacts

Availability is important to the individual customer, but will not have wide-spread impacts

Confidentiality is critical because of customer privacy issues

1.4. Category: Electricity Market

Scenario 1: Bulk Power Electricity Market

The bulk power market varies from region to region, and is conducted primarily through Regional Transmission Operators (RTO) and Independent System Operators (ISO). The market is handled independently from actual operations, although the bids into the market obviously affect which generators are used for what time periods and which functions (base load, regulation, reserve, etc.).

Therefore there are no direct operational security impacts, but there are definitely financial security impacts.

Cyber Security Requirements:

Integrity for pricing and generation information is critical

Availability for pricing and generation information is important within minutes to hours

Confidentiality for pricing and generation information is critical

Scenario 2: Retail Power Electricity Market

The retail power electricity market is still minor, but growing, compared to the bulk power market, but typically involves aggregators and energy service providers bidding customer-owned generation or load control into both energy and ancillary services. Again it is handled independently from actual power system operations. Therefore there are no direct operational security impacts, but there are definitely financial security impacts.

Cyber Security Requirements:

Integrity for pricing and generation information is critical

Availability for pricing and generation information is important within minutes to hours

Confidentiality for pricing and generation information is critical

Scenario 3: Carbon Trading Market

The carbon trading market does not exist yet, but the security requirements will probably be similar to the retail electricity market.

Cyber Security Requirements:

Integrity for pricing and generation information is critical

Availability for pricing and generation information is important within minutes to hours

Confidentiality for pricing and generation information is critical

1.5. Category: Distribution Automation

Scenario 1: Distribution Automation (DA) within Substations

Distribution SCADA System Monitors Distribution Equipment in Substations

Supervisory Control on Substation Distribution Equipment

Substation Protection Equipment Performs System Protection Actions

Reclosers in Substations

Cyber Security Requirements:

Integrity of distribution control commands is critical for distribution operations, avoiding outages, and providing power to customers reliably and efficiently

Availability for control is critical, while monitoring individual equipment is less critical

Confidentiality is not very important

Scenario 2: Distribution Automation (DA) Using Local Automation

Local Automated Switch Management

Local Volt/Var Control

Local Field Crew Communications to Underground Network Equipment

Cyber Security Requirements:

Integrity of distribution control commands is critical for distribution operations, avoiding outages, and providing power to customers reliably and efficiently.

Availability for control is critical, while monitoring individual equipment is less critical.

Confidentiality is not very important.

Scenario 3: Distribution Automation (DA) Monitoring and Controlling Feeder Equipment

• Remotely open or close automated switches	• Remotely switch capacitor banks in and out
• Remotely raise or lower voltage regulators	• Block local automated actions
• Automation of Emergency Response	• Dynamic Rating of Feeders
• Send updated parameters to feeder equipment	• Interact with equipment in underground distribution vaults
• Retrieve power system information from Smart Meters	•

Cyber Security Requirements:
Integrity of distribution control commands is critical for distribution operations, avoiding outages, and providing power to customers reliably and efficiently.

Availability for control is critical, while monitoring individual equipment is less critical.

Confidentiality is not very important.

Scenario 4: Fault Detection, Isolation, and Restoration

- The automated fault location, isolation, and service restoration function uses the combination of the power system model with the SCADA data from the field on real-time conditions to determine where a fault is probably located, by undertaking the following steps:
    1. Determines the faults cleared by controllable protective devices
    2. Determines the faulted sections based on SCADA fault indications and protection lockout signals
    3. Estimates the probable fault locations, based on SCADA fault current measurements and real-time fault analysis
    4. Determines the fault-clearing non-monitored protective device
    5. Uses closed-loop or advisory methods to isolate the faulted segment
    6. Once the fault is isolated, it determines how best to restore service to unfaulted segments through feeder reconfiguration

Cyber Security Requirements:

Integrity of outage information is critical.

Availability to detect large scale outages usually involve multiple sources of information

Confidentiality is not very important.

Scenario 5: Load Management

Load management provides active and passive control by the utility of customer appliances (e.g. cycling of air conditioner, water heaters, and pool pumps) and certain C&I customer systems (e.g. plenum pre-cooling, heat storage management).

- Direct load control and load shedding
- Demand side management
- Load shift scheduling
- Curtailment planning
- Selective load management through Home Area Networks

Cyber Security Requirements:

Integrity of load control commands is critical to avoid unwarranted outages

Availability for load control is important – in aggregate (e.g. > 300 MW), it can be critical.

Confidentiality is not very important.

Scenario 6: Distribution Analysis using Distribution Power Flow Models

The brains behind the monitoring and controlling of field devices are the DA analysis software applications. These applications generally use models of the power system to validate the raw data, assess real-time and future conditions, and issue the appropriate actions. The applications

may be distributed and located in the field equipment for local assessments and control, and/or may be centralized in a Distribution Management System for global assessment and control.

Local peer-to-peer interactions between equipment.

Normal distribution operations using the Distribution System Power Flow (DSPF) model.

Emergency distribution operations using the DSPF model.

Study-Mode Distribution System Power Flow (DSPF) model.

DSPF /DER Model of distribution operations with significant DER generation/storage.

Cyber Security Requirements:

Integrity is critical to operate the distribution power system reliably, efficiently, and safely.

Availability is critical to operate the distribution power system reliably, efficiently, and safely.

Confidentiality is not important.

Scenario 7: Distributed Energy Resource (DER) Management - Distribution Operations

In the future, more and more of generation and storage resources will be connected to the distribution network and will significantly increase the complexity and sensitivity of distribution operations. Therefore, the management of DER generation will become increasingly important in the overall management of the distribution system, including load forecasts, real-time monitoring, feeder reconfiguration, virtual and logical microgrids, and distribution planning.

Direct monitoring and control of DER.

Shut-down or islanding verification for DER.

Plug-in Hybrid Vehicle (PEV) management, as load, storage, and generation resource.

Electric storage fill/draw management.

Renewable energy DER with variable generation.

Small fossil resource management, such as backup generators to be used for peak shifting.

Cyber Security Requirements:

Integrity is critical for any management/control of generation and storage.

Availability requirements may vary depending on the size (individual or aggregate) of the DER plant.

Confidentiality may involve some privacy issues with customer-owned DER.

Scenario 8: Distributed Energy Resource (DER) Management – Control Centers

Distribution planning typically uses engineering systems with access only to processed power system data that is available from the control center. It is therefore relatively self-contained.

• Operational planning	• Assessing Planned Outages
• Storm Condition Planning	• Short-term distribution planning
• Short-Term Load Forecast	• Short-Term DER Generation and Storage Impact Studies
• Long-term distribution planning	• Long-Tem Load Forecasts by Area
• Distribution Financial Planners	• Distribution System Upgrades and Extension
• Optimal Placements of Switches, Capacitors, Regulators, and DER	

Cyber Security Requirements:

Integrity not critical due to multiple sources of data.

Availability is not important.

Confidentiality is not important.

1.6. Category: Plug In Hybrid Electric Vehicles (PHEV)

Scenario 1: Customer Connects Plug In Hybrid Electric Vehicle to Energy Portal

A customer plugging in an electric vehicle at their premise to charge its battery. Variations of this scenario will be considered that add complexity: a customer charging their vehicle at another location and providing payment or charging at another location where the premise owner pays.

Objective/Requirements:

The customer's information is kept private. Billing information is accurate

Scenario 2: Customer Connects Plug In Hybrid Electric Vehicle to Energy Portal and Participates in 'Smart' (Optimized) Charging

In addition to simply plugging in an electric vehicle for charging, in this scenario the electric vehicle charging is optimized to take advantage of lower rates or help prevent excessive load peaks on the electrical system.

Objective/Requirements:

Customer information is kept private.

Scenario 3: Plug In Hybrid Electric Vehicle or Customer Receives and Responds to Discrete Demand Response Events

- An advanced scenario for electric vehicles is the use of the vehicle to provide energy stored in its battery back to the electrical system. Customers could participate in demand response programs where they are provided an incentive to allow the utility to request power from the vehicle at times of high system load.

Objective/Requirements:

- Improved system stability and availability. To keep customer information private.

To insure DR messages are accurate and trustworthy

Scenario 4: Plug In Hybrid Electric Vehicle or Customer Receives and Responds to Utility Price Signals

The electric vehicle is able to receive and act on electricity pricing data sent from the utility. The use of pricing data for charging is primarily covered in another scenario. The pricing data can also be used in support of a distributed resource program where the customer allows the vehicle to provide power to the electric grid based on market conditions.

Objective/Requirements:

Improved system stability and availability. Pricing signals are accurate and trustworthy.

Customer information is kept private.

1.7. Category: Distributed Resources

Scenario 1: Customer Provides Distributed Resource

The process of connecting a distributed resource to the electric power system and the requirements of net metering.

Objective/Requirements:

Customer information is kept private. Net metering is accurate and timely.

Scenario 2: Utility Controls Customer's Distributed Resource

Distributed generation and storage can be used as a demand response resource where the utility can request or control devices to provide energy back to the electrical system. Customers enroll in utility programs that allow their distributed resource to be used for load support or to assist in maintaining power quality. The utility programs can be based on direct control signals or pricing information.

Objective/Requirements:

Commands are trustworthy and accurate. Customer's information is kept private.

DR messages are received timely.

1.8. Category: Transmission Operations

Scenario 1: Real-time Normal Transmission Operations Using EMS Applications and SCADA Data

Transmission normal real-time operations involve monitoring and controlling the transmission system using the SCADA and Energy Management System. The types of information exchanged include:

Monitored equipment states (open/close), alarms (overheat, overload, battery level, capacity), and measurements (current, voltage, frequency, energy) Operator command and control

actions, such as supervisory control of switching operations, setup/options of EMS functions, and preparation for storm conditions.

Closed-loop actions, such as protective relaying tripping circuit breakers upon power system anomalies.

Automation system controls voltage, var and power flow based on algorithms, real-time data, and network linked capacitive and reactive components.

Cyber Security Requirements:

Integrity is vital to the safety and reliability of the transmission system.

Availability is critical to protective relaying (e.g. < 4 ms) and operator commands (e.g. one second).

Confidentiality is not important.

Scenario 2: EMS Network Analysis Based on Transmission Power Flow Models

Energy Management Systems (EMS) assesses the state of the transmission power system using the transmission power system analysis models and the SCADA data from the transmission substations.

EMS performs model update, state estimation, bus load forecast.

EMS performs contingency analysis, recommends preventive and corrective actions.

EMS performs optimal power flow analysis, recommends optimization actions.

EMS or planners perform stability study of network.

Exchange power system model information with RTOs/ISOs and/or other utilities.

Cyber Security Requirements:

Integrity is vital to the reliability of the transmission system.

Availability is critical to react to contingency situations via operator commands (e.g. one second).

Confidentiality is not important.

Scenario 3: Real-Time Emergency Transmission Operations

During emergencies, the power system takes some automated actions and the operators can also take actions:

Power System Protection: Emergency operations handles under-frequency load/generation shedding, under-voltage load shedding, LTC control/blocking, shunt control, series compensation control, system separation detection, and wide area real time instability recovery.

Operators manage emergency alarms.

SCADA system responds to emergencies by running key applications such as disturbance monitoring analysis (including fault location), dynamic limit calculations for transformers and breakers based on real time data from equipment monitors, and pre-arming of fast acting emergency automation SCADA/EMS generates signals for emergency support by distribution utilities (according to the T&D contracts):

Operators perform system restorations based on system restoration plans prepared (authorized) by operation management.

Cyber Security Requirements:

Integrity is vital to the safety and reliability of the transmission system.

Availability is critical to protective relaying (e.g. < 4 ms) and operator commands (e.g. one second).

Confidentiality is not important.

Scenario 4: Wide Area Synchro-Phasor System

The Wide Area Synchro-Phasor system provides synchronized and time-tagged voltage and current phasor measurements to any protection, control, or monitoring function that requires measurements taken from several locations, whose phase angles are measured against a common, system wide reference. Present day implementation of many protection, control, or monitoring functions is hobbled by not having access to the phase angles between local and remote measurements. With system wide phase angle information, they can be improved and extended. The essential concept behind this system is the system wide synchronization of measurement sampling clocks to a common time reference.

Cyber Security Requirements:

Integrity is vital to the safety and reliability of the transmission system.

Availability is critical to protective relaying (e.g. < 4 ms) and operator commands (e.g. one second).

Confidentiality is not important.

1.9. Category: RTO/ISO Operations

Scenario 1: RTO/ISO Management of Central and DER Generators and Storage

RTOs and ISOs manage the scheduling and dispatch of central and distributed generation and storage.

These functions include:

Real time scheduling with the RTO/ISO (for non-market generation/storage)

Real time commitment to RTO/ISO

Real time dispatching by RTO/ISO for energy and ancillary services

Real time plant operations in response to RTO/ISO dispatch commands

Real time contingency and emergency operations.

Black Start (system restoration after blackout).

Emissions monitoring and control.

Cyber Security Requirements:

Integrity is vital to the safety and reliability of the transmission system.

Availability is critical to operator commands (e.g. one second).

Confidentiality is not important.

1.10. Category: Asset Management

Scenario 1: Utility gathers circuit and/or transformer load profiles

Load profile data is important for the utility planning staff and is also used by the asset management team that is monitoring the utilization of the assets and by the SCADA/EMS and system operations team. This scenario involves the use of field devices that measure loading, the communications network that delivers the data, the historian database and the load profile application and display capability that is either separate or an integrated part of the SCADA/EMS.

Load profile data may also be used by automatic switching applications that use load data to ensure new system configurations do not cause overloads.

Objective/Requirements:

Data is accurate (integrity).

Data is provided timely.

Customer data is kept private.

Scenario 2: Utility makes decisions on asset replacement based on a range of inputs including comprehensive off line and on line condition data and analysis applications.

When decisions on asset replacement become necessary the system operator, asset management, apparatus engineering and maintenance engineering staff work closely together with the objective of maximizing the life and utilization of the asset while avoiding an unplanned outage and damage to the equipment.

This scenario involves the use of on-line condition monitoring devices for the range of assets monitored, off line test results, mobile work force technologies, the communications equipment used to collect the on-line data, data marts (historian databases) to store and trend data as well as condition analysis applications, CMMS applications, display applications and SCADA/EMS.

Objective/Requirements:

Data provided is accurate and trustworthy.

Data is provided timely.

Scenario 3: Utility performs localized load reduction to relieve circuit and/or transformer overloads

Transmission capacity can become constrained due to a number of system level scenarios and result in an overload situation on lines and substation equipment. Circuit and/or transformer overloads at the distribution level can occur when higher than anticipated customer loads are placed on a circuit or when operator or automatic switching actions are implemented to change the network configuration. Traditional load reduction systems are used to address generation shortfalls and other system wide issues. Localized load reduction can be a key tool enabling the operator to temporarily curtail the load in a specific area to reduce the impact on specific equipment. This scenario describes the integrated use of the AMI system, the demand response system, other load reduction systems and the SCADA/EMS to achieve this goal.

Objective/Requirements:

Load reduction messages are accurate and trustworthy.

Customer's information is kept private.

DR messages are received and processed timely.

Scenario 4: Utility system operator determines level of severity for an impending asset failure and takes corrective action

When pending asset failure can be anticipated the system operator, asset management, apparatus engineering and maintenance engineering staff work closely together with the objective of avoiding an unplanned outage while avoiding further damage to the equipment.

This scenario involves the use of on-line condition monitoring devices for the range of assets monitored, off line test results, mobile work force technologies, the communications equipment used to collect the on-line data, data marts (historian databases) to store and trend data as well as condition analysis applications, CMMS applications, display applications and SCADA/EMS.

Objective/Requirements:

Asset information provided is accurate and trustworthy.

Asset information is provided timely.

APPENDIX B

1. Admin_Roles_Access: Design administrative functions such that administrative responsibilities of the system will be well defined and compartmentalized such that administrators do not automatically have access to assets, except for necessary exceptions.
2. Audit: Record in audit records: date and time of action, location of the action, and the entity responsible for the action.
3. Audit_Log_Maintenance: The audit log will be maintained in such a way as to prevent unauthorized access, modification, deletion or overflow conditions.
4. Trusted_Path&Channel: Provide a trusted path and channel between the system and a remote trusted system for the performance of security-critical operations.
5. Confidentiality: Provide high assurance that information is not disclosed to unauthorized individuals, processes, or devices.
6. Crypto_Comm_Channel: Provide secure session establishment between the system and remote systems using NSA approved confidentiality, integrity, authentication and non-repudiation of network transmissions. Restrict user access to cryptographic IT assets in accordance with a specified user access control policy. Provide complete separation between plaintext and encrypted data and between data and keys.
7. Crypto_Storage: Provide NSA approved confidentiality, integrity, authentication and non-repudiation of stored information content.
8. Crypto_Import_Export: Protect cryptographic data assets when they are being transmitted to and from the TOE, either through intervening untrusted components or directly to/from human users.
9. Import_Export_Control: Provide security services and labels on import/export data that is consistent with policy (i.e. user, data source, data content, and intended audience).
10. Fault_Tolerant: Provide fault tolerant operations for critical components and continue to operate in the presence of specific failures in one or more system components.
11. Integrity_Checks: Provide periodic integrity checks on system data, user data, and hardware/software functionality.
12. I&A: Uniquely identity and robustly authenticate each user that will support accountability and authorization.
13. Integ_Data: Ensure the integrity of system data, user data, and security attributes transferred or replicated within the system.
14. Emanantions: Limit system-produced unintended emanations (intelligible or not) to within a specified limit.
15. Isolate_Executables: Run executable code in a protected domain where the code's potential errors or malicious code will not significantly impact other system functions of other valid users of the system.

16. Maintain_Online: Provide online maintenance role with a limited capability to observe the usage of specified services or resources as necessary.
17. NonRepudiation: Provide accountability and nonrepudiation of information transfer between entities.
18. Obj_Attr: Maintain object security attributes with integrity.
19. Priority_Of_Service: Control access to resources so that lower-priority activities do not unduly interfere with or delay higher-priority activities.
20. Resource_Quotas: Use resource quotas to limit user and service use of system resources to a level that will prevent degradation or denial of service to other critical users and services.
21. Rollback: Recover from user operations by undoing some user operations (i.e., "rolling back") to restore a previous known state.
22. SW_Download: Provide the ability to update the TOE software program to patch discovered security flaws or other flaws in the program that could be exploited by the adversary. SW download is implemented with High Robustness.
23. Session_Protection: Provide protection of a user or admin session to prevent an unauthorized user from using an unattended computer where a valid user has an active session.
24. Secure_State: Maintain and recover to a secure state without security compromise after power cycle, addition or removal of components, system error or other interruption of system operation.
25. Security_Mgt: Manage the initialization of, limits on, and allowable operations on security attributes, security-critical data, and security mechanisms.
26. Security_Roles: Maintain security-relevant roles and the association of users with those roles.
27. Sys_Assur_HW/SW/FW: Ensure that security-relevant software, hardware, and firmware are correctly functioning through features and procedures.
28. Tamper: Provide system features that prevent, detect, and resist physical tampering of a system component, and use those features to limit security breaches.
29. User_Attributes: Maintain a set of security attributes (which may include group membership, clearance, access rights, etc.) associated with individual users in addition to user identity.
30. Secure_via_Cryptography: Ensure the protection provided to data in the system is predicated on the secrecy of the keys not in the secrecy of the design.
31. Malicious_Code: Incorporate malicious code prevention procedures and mechanisms.
32. Comp_Attributes: Maintain a set of security attributes associated with individual components in addition to component identity.
33. Attr_based_Policy: Provide policy based access control via security attributes on Users, Components, and Objects.

34. Admin_Guidance: Deter administrator errors by providing adequate administrator guidance.
35. Config_Management: Implement a configuration management plan. Implement configuration management to assure storage integrity, identification of system connectivity (software, hardware, and firmware), and identification of system components (software, hardware, and firmware).
36. Crypto_Key_Man: Fully define cryptographic components, functions, and interfaces. Ensure appropriate protection for cryptographic keys throughout their lifecycle, covering generation, distribution, storage, use, and destruction.
37. Secure_Configuration: Manage and update system security policy data and enforcement functions, and other security-relevant configuration data, in accordance with organizational security policies.
38. Evaluated_System: Evaluate system via Common Criteria methods for proper implementation including examination for accidental or deliberate flaws in code made by the developer. The accidental flaws could be lack of engineering detail or bad design. Where the deliberate flaws would include building trapdoors for later entry as an example.
39. Sys_Backup_Procs: Provide backup procedures to ensure that the system can be reconstructed.
40. User_Auth_Management: Manage and update user authorization and privilege data in accordance with organizational security and personnel policies.
41. User_Guidance: Provide documentation for the general user.
42. Component_Engineering: Manage lifecycle maintenance such that when component hardware becomes obsolete the AMI hardware/software is redesigned to support production
43. Admin_Available: Provide at least one Security Administrator (authorized by the U.S. or the host country) to respond to administrative issues including fixing enrollment/I&A issues.
44. Trusted_Facility: Provide a trusted facility for initialization.
45. Physical_Security: Provide an appropriate level of physical security.
46. BackhaulSLA: Negotiate an SLA with the Backhaul network that meets the operational needs of the mission. This includes required fault-tolerant aspects of the Backhaul's system including but not limited to routers, switch, and even "back-hoe" protection.
47. Enrollment_Process: Provide a registration/enrollment procedure that includes both a chain of trust of user identity to enroll (e.g. DoD PKI or a US Passport) plus a chain of trust of access and authorization to those domains to grant access.

APPENDIX C

OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data[192]

General Definition

- "data controller" means a party who, according to domestic law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf;
- "personal data" means any information relating to an identified or identifiable individual (data subject);
- "trans-border flows of personal data" means movements of personal data across national borders.

Scope of the Guidelines

These Guidelines apply to personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties.

These Guidelines should not be interpreted as preventing:

- The application, to different categories of personal data, of different protective measures depending upon their nature and the context in which they are collected, stored, processed or disseminated;
- The exclusion from the application of the Guidelines of personal data which obviously do not contain any risk to privacy and individual liberties; or
- The application of the Guidelines only to automatic processing of personal data.

Exceptions to the Principles contained in Parts Two and Three of these Guidelines, including those relating to national sovereignty, national security and public policy ("ordre public"), should be:

- As few as possible, and
- Made known to the public.

In the particular case of Federal countries the observance of these Guidelines may be affected by the division of powers in the Federation.

---

[192] http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html

These Guidelines should be regarded as minimum standards which are capable of being supplemented by additional measures for the protection of privacy and individual liberties.

Principles

1. Collection Limitation

   There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

2. Data Quality

   Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

3. Purpose Specification

   The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

4. Use Limitation

   Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

   - with the consent of the data subject; or
   - by the authority of law.

5. Security Safeguards Principle

   Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

6. Openness

   There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

7. Individual Participation Principle

   An individual should have the right:

   - to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
   - to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive;

in a reasonable manner; and
in a form that is readily intelligible to him;

- to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and
- to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

8. Accountability

   A data controller should be accountable for complying with measures which give effect to the principles stated above.

Basic Principles of International Application: free flow and legitimate restrictions:

1. Member countries should take into consideration the implications for other Member countries of domestic processing and re-export of personal data.
2. Member countries should take all reasonable and appropriate steps to ensure that trans-border flows of personal data, including transit through a Member country, are uninterrupted and secure.
3. A Member country should refrain from restricting transborder flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A Member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other Member country provides no equivalent protection.
4. Member countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection.

National Implementation

In implementing domestically the principles set forth in Parts Two and Three, Member countries should establish legal, administrative or other procedures or institutions for the protection of privacy and individual liberties in respect of personal data. Member countries should in particular endeavor to:

- adopt appropriate domestic legislation;
- encourage and support self-regulation, whether in the form of codes of conduct or otherwise;
- provide for reasonable means for individuals to exercise their rights;
- provide for adequate sanctions and remedies in case of failures to comply with measures which implement the principles set forth in Parts Two and Three; and
- ensure that there is no unfair discrimination against data subjects.

International Co-Operation

1. Member countries should, where requested, make known to other Member countries details of the observance of the principles set forth in these Guidelines. Member countries should also ensure that procedures for transborder flows of personal data and for the protection of privacy and individual liberties are simple and compatible with those of other Member countries which comply with these Guidelines.
2. Member countries should establish procedures to facilitate:
    - information exchange related to these Guidelines, and
    - mutual assistance in the procedural and investigative matters involved.
3. Member countries should work towards the development of principles, domestic and international, to govern the applicable law in the case of transborder flows of personal data.

APPENDIX D:
A Summary of Research Report on Data Protection and Role Collaboration within Organizations [193]

About the Study

The Ponemon Institute LLC independently conducted a study to understand the perceptions of three different groups of information stakeholders on how privacy and data protection risks are being managed in their organizations. The study sample included group of information security, privacy, compliance and marketing executives from a variety of industries across the public and private sectors.

1. Collaboration among security and privacy practitioners in an organization seems to reduce the risk of a compromise or breach of personal information.
    - Organizations with poor collaboration between security and privacy professionals were
        - 50% more likely to have suffered a data breach in the past two years as organizations with good collaboration.
        - 74%of those organizations indicating that collaboration among security and privacy professionals was poor reported one or more data breaches in the past 24 months.
        - 29 % of those indicating that collaboration was adequate to excellent reported one or more data breaches in the past 24 months.
2. People who collect and use data don't often consult with security and privacy professionals.
    - There appear to be significant differences of perception between executives who collect and use data and security and privacy professionals in terms of the degree of collaboration among the three roles.
    - While 78% of security and privacy professionals believe they are regularly consulted by marketing colleagues on the collection and use of data, only 30% of marketers said they actually did consult them.
    - 69%t of marketers agree or strongly agree that they rarely consult privacy or security professionals before using sensitive or confidential data,

[193] Challenges to Organizational Collaboration Could Put Stakeholders' Privacy at Risk Research Report on Data Protection and Role Collaboration within Organizations A Microsoft Corp.'s most recent Security Intelligence Report, released in October 2007

- 12% of security and privacy professionals believe they are rarely consulted.

3. Individuals responsible for safeguarding data do not share the same views as the people who collect and use data.
    - Privacy and security practitioners have vastly different views about privacy risk than professionals who collect and use data.
    - 59% of privacy and compliance practitioners and 53% of security practitioners believe that the safeguarding of personal information is well-coordinated within their organizations, however only 32% of people who collect and use data believe this to be true.
    - 45% of information security professionals and 32% of privacy and compliance professionals believe that privacy objectives are not in conflict with business objectives, while only 21% percent of people who collect and use data believe that such conflicts do not exist.
    - 50% of information security professionals and 39% of privacy and compliance professionals believe that business opportunities cannot be achieved without good privacy practices, when only 18 percent of marketers believe this is true.
    - The above statistics suggests that the individuals responsible for information protection and those, such as marketers, who use personal and sensitive data to achieve business objectives, may not share the same understanding about information risk management.
4. Security and privacy professionals believe negligence in data use and sharing is the biggest threat to data protection practices.
    - 50% of privacy and compliance professionals and 35% of information security professionals cited negligence and mistakes in data use and sharing as the top risk, while only 45% of professionals who use and collect data fear phishing attacks.
5. Privacy and security practitioners are aligned in their perceptions that companies are at risk if data protection practices are lax.
    - Marketers perceive that insufficient or inaccurate personal information for business use puts companies at risk and therefore there seems to be conflicting perceptions about what causes data protection risk in an organization.
6. Preserving or enhancing an organization's reputation and trust is important, especially for professionals who collect and use data.
    - 65% or more professionals who collect and use data in all countries believe that "the preserving or enhancing the organization's reputation and trust" is among the most important business drivers for data protection, when only 49% of privacy and compliance professionals and 23% of information security

professionals say that reputation and trust are among the most important business drivers for data protection.

- Avoiding threats is the top business driver for security professionals, and regulatory compliance is the top driver for privacy and compliance professionals.
- This indicates that security and privacy professionals will benefit from communicating the reputation and trust impacts associated with a lack of focus on avoiding threats of managing compliance.

7. Who has the most influence over the company's data protection practices?
    - Each functional group sees itself as being more important to determining data protection practices in their organizations. For example,
    - 33% of information security professionals see themselves as most influential,
    - 21% of professionals who collect and use data consider information security professionals as most influential in determining data protection practices, and
    - 33% of privacy and compliance professionals see themselves as most influential,
    - 16% of information security professionals see privacy and compliance as being most influential.

It appears that business units and professionals not in the privacy and security functions who collect and use data have much more influence in the U.S. than in Europe. Where

- 47 % of respondents in the U.S. say that business units have the most influence,
- 25% of respondents in the U.K. and
- 33% in Germany believe that business units are most influential.

The perception of influence appears to vary by function and location, thus making it difficult to assign overall accountability and responsibility.

8. Organizations where there is a lack of effective collaboration and a higher incidence of data breach have a strong desire to formally combine privacy and security roles.
    - The degree of collaboration that already exists among security and privacy professionals and the reported incidence of data breaches appear to have significant influence over their desire to formally combine their respective roles to achieve improved governance over sensitive data.
    - 52% of those polled who reported a reasonable level of collaboration between security and privacy professionals were supportive of formally combining their responsibilities under common management. Conversely, where collaboration was reported as poor, and
    - 80% or more of respondents indicated a strong desire to formally combine the roles.

9. Differences in regulations and how personal data is defined affect perceptions on how privacy risks should be managed.
    - 55% of respondents in the U.K and
    - 48% of respondents in Germany say "achieving regulatory and legal compliance is the most important driver for data protection. "While
    - 35% of respondents in the U.S. believe regulatory and legal compliance is among the most important business drivers for data protection.
    - The most important business driver for the U.S. is avoiding external attacks and insider threats, but is the third most important business driver for data protection in both the U.K. and Germany.
    - The importance of preventing attacks and insider threats among U.S. respondents could be related to the study's finding that the frequency of reported data breaches is lower in both the U.K. and Germany.

Implications for Business

Microsoft believes that there are significant benefits to organizations that take a holistic approach to the management of privacy risks by:

1. Understanding how the three organizational groups closest to the protection and use of personal information perceive the current state of privacy risk in their organization and what the ideal state would be. This study provides some insight for such understanding.
2. The next step is for organizations to involve privacy, security and marketing practitioners in creating a strategic and holistic approach to privacy risk.

The study's findings reveal that although people who collect and use customer information recognize the value in protecting trust in their organization, their perceptions and behaviors often are at odds with those of privacy and security professionals. This suggests that organizations need to develop a common understanding among the various parties interested in the use and protection of data about how to safeguard personal information while not impede business objectives.